Tweede Kamer der Staten-Generaal 2

Vergaderjaar 2015–2016

# 34 388 Regels over het verwerken van gegevens ter bevordering van de veiligheid en de integriteit van elektronische informatiesystemen die van vitaal belang zijn voor de Nederlandse samenleving en regels over het melden van ernstige inbreuken (Wet gegevensverwerking en meldplicht cybersecurity)

## Nr. 3 MEMORIE VAN TOELICHTING

## ALGEMEEN

### 1. Inleiding

Dit wetsvoorstel introduceert een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna ook: ICT-inbreuken) en stelt regels over het verwerken van gegevens ten behoeve van de taken van de Minister (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) van Veiligheid en Justitie op het terrein van cybersecurity.

De meldplicht geldt alleen voor zogenoemde vitale aanbieders: overheidsorganisaties en privaatrechtelijke rechtspersonen die producten of diensten aanbieden waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse samenleving. De meldplicht geldt daarnaast alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van dergelijke producten of diensten in belangrijke mate wordt of kan worden onderbroken. De meldplicht geldt uitsluitend voor bij algemene maatregel van bestuur aan te wijzen (categorieën van) vitale aanbieders van daarbij aan te wijzen producten of diensten. De melding moet worden gedaan aan de Staatssecretaris van Veiligheid en Justitie. De melding wordt behandeld door het Nationaal Cyber Security Centrum (NCSC), een onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), die deel uitmaakt van het Ministerie van Veiligheid en Justitie.[1] De melding stelt het NCSC in staat om hulp te verlenen aan de getroffen aanbieder en om andere aanbieders te waarschuwen, met als uiteindelijke doel om het risico van maatschappelijke ontwrichting in te schatten en die ontwrichting te voorkomen of in elk geval zo veel mogelijk te beperken.

[1] In dit wetsvoorstel worden taken en bevoegdheden toegekend aan de Minister (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) van Veiligheid en Justitie, en niet rechtstreeks aan het NCSC. Waar deze memorie van toelichting de rol van het NCSC bespreekt, wordt, tenzij uit de context anders volgt, gedoeld op de uitvoering van de taken en bevoegdheden van de Staatssecretaris.

kst-34388-3
ISSN 0921 - 7371
's-Gravenhage 2016

Deze meldplicht voor ICT-inbreuken is aangekondigd in een brief aan de Tweede Kamer van 6 juli 2012,[2] naar aanleiding van een verzoek van de Kamer om te komen tot de wettelijke vastlegging van een «security breach notification» bij het NCSC voor organisaties die betrokken zijn bij voor de samenleving vitale informatiesystemen.[3] Aanleiding voor dat verzoek was de elektronische inbraak bij het bedrijf DigiNotar in het najaar van 2011. Deze ICT-inbreuk heeft het toegenomen belang en de onderlinge verwevenheid van ICT-systemen bij de overheid en (overige) vitale sectoren zichtbaar gemaakt. De meldplicht sluit aan bij het voorstel van de Europese Commissie om EU-breed te komen tot een meldplicht voor overheden en vitale marktpartijen die bijdraagt aan het verhogen van de digitale veiligheid.[4]

Naar aanleiding van het Pobelka-incident in 2013[5] is daarnaast onderzocht of er voldoende rechtsbasis is voor de verwerking van gegevens door het NCSC. In de brief van 12 december 2013 is de Tweede Kamer bericht dat voor de huidige verwerking van (persoons)gegevens door het NCSC een afdoende wettelijke grondslag voorhanden is, maar dat het aangewezen is om de taken van het NCSC in het kader waarvan persoonsgegevens worden verwerkt, alsook de daaraan gekoppelde bevoegdheid tot verwerking daarvan, van een steviger wettelijke grondslag te voorzien.[6] Daartoe strekken met name de artikelen 2 en 3 van dit wetsvoorstel. In dezelfde brief is tevens ingegaan op het belang van de vertrouwelijkheid van aan het NCSC verstrekte gegevens.[7] Om die vertrouwelijkheid te waarborgen, bevat het voorgestelde artikel 9 een strikte regeling over de verstrekking aan derden van door het NCSC verkregen vertrouwelijke gegevens.

Het begrip vitale aanbieder zoals dat wordt gebruikt in dit wetsvoorstel, omvat zowel overheidsorganisaties als privaatrechtelijke rechtspersonen. Onder vitale aanbieders worden zowel vitale aanbieders die onder de meldplicht vallen (aangewezen vitale aanbieders) als andere vitale aanbieders verstaan. Overigens is de doelgroep van het NCSC breder dan alleen vitale aanbieders: het NCSC richt zich ook op de niet-vitale aanbieders die onderdeel zijn van de rijksoverheid.

## 2. Meldplicht

### *2.1. Inleiding*

Doel van de in dit wetsvoorstel vervatte meldplicht voor aangewezen vitale aanbieders aan het NCSC is tweeledig. Een melding van een ernstige ICT-inbreuk bij een dergelijke aanbieder aan het NCSC is enerzijds bedoeld om tijdig te kunnen inschatten hoe groot de impact en daarmee de potentiële maatschappelijke ontwrichting van een ICT-inbreuk is. Anderzijds stelt de melding het NCSC in staat om hulp aan de getroffen organisatie te verlenen en om te anticiperen op de mogelijk bredere effecten van een dergelijke inbreuk, met name ook door andere vitale aanbieders alsook andere van de rijksoverheid deel uitmakende aanbieders te waarschuwen en te adviseren. Vastlegging van deze meldplicht in de wet benadrukt het maatschappelijk belang van bovenge-

---

[2] Kamerstukken II 2012/13, 26 643, nr. 247.

[3] Motie-Hennis-Plasschaert c.s., Kamerstukken II 2011/12, 26 643, nr. 202.

[4] Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM (2013) 48 final, 2013/0027 (COD), 7 februari 2013. Zie ook Kamerstukken I 2013/14, 33 602, C.

[5] Kamerstukken II 2012/13, 26 643, nr. 272.

[6] Kamerstukken II 2013/14, 26 643, nr. 297, p. 3.

[7] Idem, p. 3 en 4.

noemde meldingen, wat naar mijn verwachting zal leiden tot een vergroting van de meldingsbereidheid van vitale aanbieders. De hulp door het NCSC aan de getroffen organisatie beoogt het bieden van handelingsperspectief door het geven van advies en informatie en waar noodzakelijk het bieden van technische ondersteuning om de gevolgen van een ICT-inbreuk te beperken en een volgende ICT-inbreuk te voorkomen.

Belangrijk bij de in dit wetsvoorstel vervatte meldplicht is ook dat deze een cultuur tracht te realiseren waarin het gezamenlijk bijdragen aan veiligheid centraal staat. In de luchtvaartsector bestaat bijvoorbeeld ruime ervaring met deze praktijk onder de noemer van het werken aan een *just culture*. De luchtvaartsector laat zien dat het bewerkstelligen van een dergelijke cultuur hand in hand kan gaan met een wettelijke meldplicht. Om een dergelijke cultuur te bevorderen is het bij het doen van de melding wel van belang dat deze in vertrouwen gedaan kan worden om kwetsbaarheden te beperken dan wel in de toekomst te vermijden. De meldplicht past qua karakter daarbij in het bredere kader van privaat-publieke samenwerking met betrekking tot het realiseren van cybersecurity binnen de rijksoverheid en de private vitale sectoren zoals uiteengezet in de tweede Nationale Cyber Security Strategie.[8]

Om het NCSC een ondersteunende rol te laten vervullen bij het voorkomen en beperken van onderbrekingen van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale diensten en producten én ter bevordering van een veiligheidscultuur waarbij meldingen gedaan worden om daar lering uit te trekken, is het voorts van belang om de drempel om meldingen te doen zo laag mogelijk te maken. Mede in verband hiermee stel ik voor om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties, zie ook de paragrafen 2.7 en 2.9). De meldplicht is primair gericht op het bieden van hulp. Het NCSC kan daarbij functioneren als informatieknooppunt om partijen te informeren en te adviseren over de te ondernemen acties. Het NCSC kan daarbij putten uit een omvangrijk nationaal en internationaal netwerk van o.a. publieke en private computercrisisteams (Computer Emergency Response Teams (CERT's) of Computer Security Incident Response Teams (CSIRT's)). Binnen de computercrisisteams is veel kennis beschikbaar over de wijze van omgaan met en het leveren van response bij ICT-inbreuken.

### *2.2. Inhoud van de melding*

Gezien het doel van de meldplicht is het van belang dat de melding, hoewel deze qua aard per vitale sector verschilt, in elk geval bestaat uit een aantal elementen. Deze zijn opgesomd in artikel 6. Ten eerste dient de melding inzicht te geven in de aard en omvang van de ICT-inbreuk. Op basis van deze informatie kan onder meer gericht in het nationale en internationale netwerk gezocht worden naar relevante informatie en kennis die voor de getroffen partij van belang is. Een specificatie van het soort getroffen systemen is in dit verband bijvoorbeeld van belang. Ten tweede dient bij de melding aangegeven te worden wat het vermoedelijke tijdstip van aanvang van de betrokken ICT-inbreuk is. Ten derde dient de melding, voor zover aan de orde, in te gaan op de reeds getroffen of te nemen maatregelen, zodat mede op basis daarvan geadviseerd kan worden over de eventuele nog te treffen aanvullende maatregelen. Ook is het van belang dat de melding ingaat op de te verwachten hersteltijd én dat de melding contactgegevens van de betrokken partij bevat, zodat desgewenst in nader contact kan worden getreden in het kader van de hulpverlening. De initiële melding kan beknopt zijn: liever een snelle

[8] Kamerstukken II 2013/14, 26 643, nr. 291.

melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten. Zo nodig kan ten behoeve van de beoordeling of en in welke zin door het NCSC aan de meldende aanbieder bijstand dient te worden verleend, alsook de inschatting van de risico's van de gemelde inbreuk voor systemen van andere aanbieders, nadere informatie worden gevraagd van de betrokken aanbieder (artikel 7).

Bij de formulering van het voorgestelde artikel 6 is aansluiting gezocht bij reeds bestaande meldplichten, teneinde de (administratieve) lasten voor aangewezen vitale aanbieders die moeten voldoen aan meerdere meldplichten zo veel mogelijk te beperken. Zie hierover ook paragraaf 2.5.

*2.3. Meldplichtige partijen*

Dit wetsvoorstel bevat een meldplicht voor die vitale aanbieders (overheid en private sector) waarbij een ICT-inbreuk direct of indirect (cascade-effect) kan leiden tot maatschappelijke ontwrichting. De (categorieën van) vitale aanbieders en hun concrete producten of diensten waarvoor de meldplicht gaat gelden, zullen worden aangewezen bij algemene maatregel van bestuur. De aanwijzing zal, zoals eerder aan uw Kamer gemeld, in ieder geval zien op vitale aanbieders in de volgende sectoren: elektriciteit, gas, drinkwater, telecom, financiën, overheid (waaronder in ieder geval primaire waterkeringen) en transport (mainports Rotterdam en Schiphol) alsook op vitale aanbieders in de sector nucleair.[9] Te denken valt daarbij aan vitale aanbieders zoals energienetwerkbeheerders, drinkwater-bedrijven, telecombedrijven, banken en Rijkswaterstaat als beheerder van primaire waterkeringen.

*2.4. Te melden ICT-inbreuken*

De meldplicht in dit wetsvoorstel ziet alleen op een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem. Van een inbreuk op de veiligheid kan bijvoorbeeld worden gesproken in het geval een niet-geautoriseerd persoon zich ongeoorloofd toegang heeft verschaft, of zelfs onopzettelijk toegang heeft verkregen, tot het computersysteem of netwerk van de vitale aanbieder. Van een verlies van integriteit kan bijvoorbeeld worden gesproken wanneer een derde in staat is geweest om, ongeoorloofd, informatie die een belangrijke rol speelt in een vitale dienst of een vitaal product toe te voegen, aan te passen of te verwijderen. Incidenten waarbij sprake is van een interne fout van een medewerker vallen over het algemeen niet onder de meldplicht, tenzij deze fout ertoe heeft geleid dat een persoon daardoor van buitenaf ongeoorloofd toegang heeft verkregen tot het systeem van de meldplichtige organisatie.

Een aangewezen vitale aanbieder is niet verplicht om elke ICT-inbreuk aan het NCSC te melden. De verplichting tot melden geldt alleen als de inbreuk tot gevolg heeft of kan hebben dat de beschikbaarheid of betrouwbaarheid van het aangewezen product of de aangewezen dienst in belangrijke mate wordt of kan worden onderbroken. Dit zou namelijk kunnen leiden tot maatschappelijke ontwrichting. In overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt wat voor de verschillende betrokken producten en diensten moet worden verstaan onder «in belangrijke mate», zo mogelijk in de vorm van meetbare drempelwaarden. Daarbij zal mede bepalend zijn onder welke

[9] Kamerstukken II 2011/12, 26 643, nr. 247, p. 3. Zie ook de «Herijkte lijst vitale infrastructuur», Kamerstukken II 2014/15, 30 821, nr. 23, p. 5.

omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Deze criteria kunnen bijvoorbeeld worden vastgelegd in richtsnoeren.

De in dit wetsvoorstel geïntroduceerde meldplicht ziet niet op verstoringen waarbij geen sprake is van een ICT-inbreuk, zoals DDoS-aanvallen (Distributed Denial of Service). Bij een DDoS-aanval wordt de bereikbaarheid van een online-dienst aangetast zonder aantasting van de systemen die in dat verband worden gebruikt. Het is wenselijk om de meldplicht te beperken tot (potentieel) ontwrichtende situaties waarbij rechtstreekse betrokkenheid van het NCSC voldoende meerwaarde heeft. Dit is niet het geval bij een DDoS-aanval, gezien het relatief eenvoudige karakter daarvan. Veelal zal het bij deze aanvallen om een tijdelijke beperking van de bereikbaarheid gaan. Hierdoor is de maatschappelijk ontwrichtende werking in deze gevallen in het algemeen veel beperkter dan bij een ICT-inbreuk. Een en ander laat overigens onverlet dat partijen de mogelijkheid hebben om ook deze verstoringen van de bereikbaarheid op basis van vrijwilligheid aan het NCSC te melden.

*2.5. Verhouding tot sectorale meldplichten*

Voor enkele sectoren geldt thans voor ICT-inbreuken al een verplichting tot melding aan de sectorale toezichthouder. Een voorbeeld hiervan is de plicht voor aanbieders van openbare elektronische communicatienetwerken en -diensten om een inbreuk op de veiligheid en een verlies van integriteit te melden aan de Minister van Economische Zaken bij het Agentschap Telecom op grond van artikel 11a.2 van de Telecommunicatiewet, als door die inbreuk of dat verlies de continuïteit van het netwerk of de dienst in belangrijke mate werd onderbroken.

Het karakter van de meldplicht bij (sectorale) toezichthouders, die tot doel heeft om de toezichthouder in staat te stellen diens taak van het houden van toezicht op de naleving van wettelijke zorgplichten te vervullen, verschilt wezenlijk van het karakter van de meldplicht aan het NCSC, die tot doel heeft het voor het NCSC mogelijk te maken om hulp te verlenen aan de getroffen organisatie en om andere organisaties die vergelijkbare risico's lopen te informeren teneinde maatschappelijke ontwrichting te voorkomen of te beperken. Ook als een vitale aanbieder een ICT-inbreuk op basis van andere wetgeving reeds moet melden bij een ander overheidsorgaan, is het cruciaal dat die aanbieder de inbreuk óók onverwijld en rechtstreeks aan het NCSC meldt, om vertraging in het daar waar nodig bieden van hulp zo veel mogelijk te beperken en om het delen van informatie over de kwetsbaarheid met andere organisaties die mogelijk getroffen zijn of worden te bespoedigen.[10] Bovendien heb ik als coördinerend bewindspersoon voor cybersecurity een eigen verantwoordelijkheid om de digitale weerbaarheid van de Nederlandse samenleving te versterken en maatschappelijke ontwrichting door het uitvallen van vitale systemen te voorkomen.

Een toename van de administratieve lasten voor vitale aanbieders die zowel op basis van huidige wetgeving als op grond van dit wetsvoorstel tot melding verplicht zullen zijn, zal zo veel mogelijk worden voorkomen. Zo zal de meldplicht ingevolge dit wetsvoorstel beperkt blijven tot ICT-inbreuken die een serieuze bedreiging voor de Nederlandse samenleving inhouden, waardoor naar verwachting geen grote aantallen incidenten gemeld zullen moeten worden. Daarnaast is de opsomming van de te verstrekken gegevens in dit wetsvoorstel globaal gehouden, en afgestemd op reeds bestaande meldplichten, waardoor het voldoen aan

[10] Zoals ook gevraagd in de motie-Hennis-Plasschaert c.s., Kamerstukken II 2011/12, 26 643, nr. 202.

de verschillende meldplichten voor de betrokken vitale aanbieder niet onnodig belastend is, daar deze grotendeels dezelfde gegevens dient aan te leveren bij de verschillende instanties die de meldingen in behandeling nemen. Ook laat dit wetsvoorstel ruimte voor maatwerk doordat na de initiële melding in contact kan worden getreden met de getroffen organisatie en waar nodig aanvullende gegevens kunnen worden opgevraagd. Om dat laatste mogelijk te maken, verplicht het voorgestelde artikel 7 de aangewezen vitale aanbieder die een inbreuk heeft gemeld om desgevraagd nadere gegevens te verstrekken die voor het NCSC nodig zijn om de risico's voor andere aanbieders in te schatten en de getroffen aanbieder bij te staan bij het treffen van maatregelen om de beschikbaarheid of betrouwbaarheid van diens product of dienst te waarborgen of te herstellen. Mede dankzij die bepaling kan de initiële melding beknopt zijn (liever een snelle melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten), en kan ad hoc worden bepaald of de inbreuk ernstig genoeg is voor (nadere) betrokkenheid van het NCSC. Daarnaast zal, waar mogelijk en wanneer de betrokken organisatie hier toestemming voor geeft, overleg plaatsvinden met toezichthouders om adviezen van het NCSC en aanwijzingen of ander handhavend optreden van de toezichthouder zo veel mogelijk op elkaar af te stemmen. Zie hiervoor ook paragraaf 4 over vertrouwelijkheid.

Het voorgaande sluit niet uit dat een getroffen organisatie in een concreet geval kan worden geconfronteerd met een aanwijzing van een toezichthouder die tegenstrijdig is aan het advies van het NCSC, bijvoorbeeld omdat in een concreet geval onvoldoende tijd beschikbaar is voor onderling overleg of omdat de betrokken organisatie voor dat overleg geen toestemming heeft gegeven. In een dergelijk geval prevaleert de aanwijzing van de toezichthouder. Het NCSC vervult geen toezichthoudende rol (zie paragraaf 2.1, laatste alinea) en zijn adviezen zijn niet bindend.

De voorgestelde meldplicht treedt niet in de thans geldende sectorale bevoegdheden. Daarmee laat de voorgestelde meldplicht ook de bestaande crisisbeheersingsstructuren onverlet.

*2.6. Verhouding tot meldplicht datalekken*

Vanaf 1 januari 2016 geldt een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens («meldplicht datalekken»).[11] Die melding moet worden gedaan aan de Autoriteit persoonsgegevens en ziet op inbreuken op de in de Wbp voorgeschreven beveiliging van persoonsgegevens tegen verlies en onrechtmatige verwerking (artikel 13 Wbp). Een vergelijkbare meldplicht voor inbreuken op de beveiliging van persoonsgegevens is reeds opgenomen in artikel 11.3a van de Telecommunicatiewet.

Bij een inbreuk op de veiligheid of een verlies van integriteit waarop het onderhavige wetsvoorstel ziet, is er weliswaar sprake van een inbreuk op de beveiliging van een informatiesysteem van een organisatie, maar daarbij hoeven niet noodzakelijkerwijs ook persoonsgegevens in het geding te zijn, bijvoorbeeld als het elektronische informatiesysteem een fysiek proces aanstuurt. De meldplicht in dit wetsvoorstel heeft daarmee een bredere reikwijdte dan de voorgestelde meldplicht op grond van de Wbp. Wanneer echter óók persoonsgegevens in het geding zijn door de ICT-inbreuk, zal de vitale aanbieder de inbreuk zowel bij het NCSC als bij de Autoriteit persoonsgegevens moeten melden.

---

[11] Artikel 34a Wet bescherming persoonsgegevens, Stb. 2015, 230 en 281.

*2.7. Verhouding tot EU-richtlijn netwerk- en informatiebeveiliging*

In februari 2013 publiceerde de Europese Commissie een Europese Cyber Security Strategie en een voorstel voor een EU-richtlijn over netwerk- en informatiebeveiliging (NIB-richtlijn).[12] Nu onlangs in de Europese onderhandelingen over deze richtlijn een akkoord is bereikt, zal de richtlijn naar verwachting binnenkort worden vastgesteld. Na publicatie (naar verwachting in het voorjaar van 2016) hebben de lidstaten nog ruim 21 maanden voor de implementatie (plus nog zes maanden voor het aanwijzen van aanbieders van vitale diensten). De richtlijn strekt tot het geven van een impuls aan het waarborgen van een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging. Met deze richtlijn wordt beoogd de beveiliging van het internet en de particuliere netwerken en informatiesystemen te verbeteren door de lidstaten ertoe te verplichten hun paraatheid te verbeteren, beter met elkaar samen te werken en door aanbieders van vitale diensten te verplichten adequate beveiligingsmaatregelen te nemen en ernstige incidenten aan de nationale bevoegde autoriteiten te rapporteren. Voorts introduceert de NIB-richtlijn een stelsel van toezicht en handhaving op deze zorgplichten en meldplicht.
Bij de implementatie van de richtlijn zal het stelsel van Nederlandse meldplichten op onderdelen moeten worden aangepast of aangevuld. Wat dat laatste betreft valt bijvoorbeeld te denken aan het stellen van eisen aan de beveiliging van informatiesystemen en aan de handhaving van die eisen en van de meldplichten. De meldplicht in dit wetsvoorstel is niet in strijd met de meldplicht van de richtlijn. Implementatie van alle verplichtingen van de richtlijn, zoals het stellen van beveiligingseisen en het regelen van toezicht en handhaving, vergt keuzes die veel overleg vragen en tijd kosten, onder meer vanwege het grote aantal betrokken sectoren en de diversiteit ervan. Intussen wordt de samenleving steeds afhankelijker van elektronische informatiesystemen, die bovendien onderling verweven zijn. Om cascade-effecten te voorkomen is het cruciaal dat aanbieders van vitale diensten het NCSC tijdig op de hoogte stellen van ernstige ICT-inbreuken. Het belang van de meldplicht voor de Nederlandse samenleving rechtvaardigt de introductie van een wettelijke regeling vooruitlopend op de implementatie van de richtlijn. Dat doet ook recht aan de aanvaarding door de Tweede Kamer, eind 2011, van de motie-Hennis-Plasschaert c.s., die de concrete aanleiding voor het opstellen van dit wetsvoorstel vormt.[13] Zie voorts de overwegingen in paragraaf 2.9. Uiteraard zal Nederland zich houden aan zijn Europeesrechtelijke verplichtingen, waaronder de tijdige implementatie van de NIB-richtlijn en het verbod om tijdens de implementatietermijn nationale maatregelen vast te stellen die het door de richtlijn voorgeschreven resultaat ernstig in gevaar kunnen brengen.

*2.8 Verhouding tot EU-Verordening elektronische identificatie en vertrouwensdiensten voor elektronische transacties (eIDAS)*

Op 1 juli 2016 treedt de zogenoemde eIDAS-verordening in werking.[14] Die verordening heeft betrekking op gekwalificeerde en niet-gekwalificeerde vertrouwensdienstverleners. Daaronder vallen ook dienstverleners die digitale certificaten afgeven, waartoe in het verleden bijvoorbeeld DigiNotar behoorde. In de verordening is met rechtstreekse werking een

---

[12] Voorstel voor een Richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, COM (2013) 48 final, 2013/0027 (COD), 7 februari 2013. Zie ook Kamerstukken I 2013/14, 33 602, C.

[13] Kamerstukken II 2011/12, 26 643, nr. 202.

[14] Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, PbEU 2014, L 257.

meldplicht geregeld aan het toezichthoudende orgaan in de zin van de verordening, en, waar passend, andere relevante organen zoals het bevoegde nationale orgaan voor informatieveiligheid of de gegevensbeschermingsautoriteit. Het voornemen is om voor Nederland uitsluitend de Staatssecretaris van Veiligheid en Justitie (als verantwoordelijke voor het NCSC) aan te merken als het bevoegde nationale orgaan voor informatieveiligheid. In het kader van de omzetting van de verordening wordt de daarin geregelde meldplicht specifiek nader bezien op de verhouding met dit wetsvoorstel. Daarbij wordt onder meer bezien of private aanbieders van vertrouwensdiensten beschouwd moeten worden als vitale aanbieder in de zin van dit wetsvoorstel.

*2.9. Naleving*

Zoals ik in paragraaf 2.1 al heb opgemerkt, stel ik voor om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties). Toezicht en sancties worden voorgeschreven in de NIB-richtlijn (zie paragraaf 2.7), maar zien daar niet alleen op de meldplichten bij verschillende overheidsinstanties, maar ook op de plicht voor aanbieders om hun informatiesystemen voldoende te beveiligen. De richtlijn laat het aan de lidstaten over om te bepalen bij welke overheidsinstantie belangrijke incidenten gemeld moeten worden en welke instantie of instanties wordt of worden belast met het toezicht op de naleving van de diverse verplichtingen uit de richtlijn en met de handhaving daarvan. Implementatie van deze onderdelen van de richtlijn vergt keuzes die veel overleg vragen en tijd kosten, onder meer vanwege het grote aantal betrokken sectoren en de diversiteit ervan. Om dit proces efficiënt vorm te geven, geef ik er de voorkeur aan de wettelijke regeling van toezicht en handhaving op de verschillende genoemde plichten, waaronder de meldplicht bij het NCSC, in onderlinge samenhang ter hand te nemen in het kader van de implementatie van de NIB-richtlijn. Met de voorgestelde wettelijke regeling voor het melden van ICT-inbreuken bij het NCSC wordt daarop vooruitlopend een concrete stap gezet. Mede vanwege de aansluiting bij de bestaande publiek-private samenwerking verwacht ik dat deze meldplicht goed zal worden nageleefd. Het nut en de noodzaak van het delen van vertrouwelijke gegevens met betrekking tot ICT-inbreuken die ernstige gevolgen hebben of kunnen krijgen, worden binnen de doelgroep breed gedragen, en de bereidheid om te melden zal door de wettelijke regeling naar mijn verwachting verder toenemen. Tegenover de bescheiden kosten van melding voor de betrokken organisaties staan hoge baten in de vorm van schadebeperking en probleemoplossing. Gegevens die ter uitvoering van de meldplicht worden verstrekt, worden door het NCSC zo vertrouwelijk mogelijk behandeld teneinde onder meer schade aan de reputatie of de concurrentiepositie van de getroffen organisatie zo veel mogelijk te voorkomen, zie artikel 9.

Wanneer mocht blijken dat een getroffen organisatie op grond van het door het NCSC verstrekte advies geen of onvoldoende maatregelen treft om (verdere) verstoring van de betrouwbaarheid of beschikbaarheid van de getroffen producten of diensten te voorkomen, kan ik ertoe besluiten de voor de betreffende sector verantwoordelijke bewindspersoon op de hoogte te brengen van het advies van het NCSC en het achterwege blijven van het nemen van adequate maatregelen, teneinde hem in staat te stellen daar waar nodig passend invulling te geven aan zijn sectorale verantwoordelijkheid. Zie in dit verband ook artikel 9.

## 3. Wettelijke grondslag voor taken en gegevensverwerking NCSC

Het NCSC ontwikkelt zich door zijn rol als nationaal kennis- en expertisecentrum op het gebied van digitale veiligheid steeds verder tot kennisknooppunt over en centraal meldpunt voor cyberincidenten. Het NCSC groeit gestaag door van nationale CERT tot Nationaal Cybersecurity Operations Centre (NCSOC). Ontwikkelingen zoals de facilitering van Information Sharing and Analysis Centres (ISAC's) en de opzet van een nationaal responsnetwerk laten zien dat het NCSC een steeds belangrijkere rol speelt in het bevorderen van de vitale digitale infrastructuren in Nederland. De doelgroep van het NCSC bestaat, zoals hierboven ook al aangegeven (paragraaf 1, laatste alinea), uit de vitale aanbieders (overheid en private sector) en andere (niet-vitale) aanbieders die deel uitmaken van de rijksoverheid.

Bij de uitvoering van zijn taken verwerkt het NCSC een veelheid aan gegevens, waaronder ook persoonsgegevens. Bij de verwerking van persoonsgegevens gaat het daarbij in beginsel alleen om die gegevens die noodzakelijk zijn voor het uitoefenen van de in artikel 2 van dit wetsvoorstel omschreven taken, zoals de bij een incident of dreiging betrokken IP-adressen,[15] e-mailadressen en domeinnamen,[16] alsook contactgegevens van overheids- en vitale private partijen. Zie voor een nadere toelichting hierop ook paragraaf 6 van deze memorie. Op de verwerking van genoemde persoonsgegevens door het NCSC is de Wet bescherming persoonsgegevens (Wbp) van toepassing. De Autoriteit persoonsgegevens en de departementale functionaris voor de gegevensbescherming houden toezicht op deze verwerkingen van persoonsgegevens door het NCSC. De Wbp vereist voor iedere verwerking van persoonsgegevens dat deze kan worden gebaseerd op een van de grondslagen van artikel 8 Wbp. Zoals de Minister van Veiligheid en Justitie in zijn brief van 12 december 2013 heeft uiteengezet, is het wenselijk om de wettelijke grondslag voor gegevensverwerking door het NCSC, gelet op het groeiend belang en de ontwikkeling van het NCSC, te verstevigen.[17]

Ten behoeve van die versteviging voorziet dit wetsvoorstel in een vastlegging van de NCSC-taken in het kader waarvan persoonsgegevens kunnen worden verwerkt (zoals de analyse ten behoeve van advisering en ondersteuning bij incidenten of dreigingen, zie hierna), alsook in samenhang hiermee in een steviger wettelijke grondslag voor de bevoegdheid tot die verwerking (artikelen 2 en 3). Voorts voorziet dit wetsvoorstel volledigheidshalve met het oog op dezelfde taken ook in een concrete wettelijke basis voor het verwerken van andere gegevens (bijvoorbeeld over «malware» (kwaadaardige software) of kwetsbaarheden, eveneens in de artikelen 2 en 3). Ook voorziet dit wetsvoorstel in een wettelijke grondslag om bijvoorbeeld bij andere publiekrechtelijke organisaties de voor bovengenoemde taakuitoefening noodzakelijke gegevens te vragen en in de mogelijkheid van die derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan het NCSC (artikel 4). Ten slotte regelt dit wetsvoorstel de voorwaarden waaronder vertrouwelijke gegevens die bij het NCSC berusten, verstrekt mogen worden aan derden (artikel 9).

---

[15] Het IP-adres is een nummer waarmee een computer met internetverbinding kan worden geïdentificeerd. IP-adressen worden door de Autoriteit persoonsgegevens over het algemeen als persoonsgegeven aangemerkt, zie *Cbp Richtsnoeren – Publicaties van persoonsgegevens op het internet*, 2007, p. 10.

[16] Een domeinnaam kan een persoonsgegeven zijn, bijvoorbeeld als de naam van de beheerder van de website deel uitmaakt van de domeinnaam.

[17] Kamerstukken II 2013/14, 26 643, nr. 297, p. 3.

Een belangrijk doel van de NCSC-taken (zie de aanhef van artikel 2, eerste lid) is de voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van elektronische informatiesystemen van vitale aanbieders (overheid en private sector) en van andere aanbieders die deel uitmaken van de rijksoverheid. Ten behoeve van dat doel heeft het NCSC verschillende taken in het kader waarvan onder meer persoonsgegevens worden verwerkt. Het gaat hierbij allereerst om het bijstaan van deze aanbieders bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van de betrokken producten of diensten te waarborgen of te herstellen én om het informeren en adviseren van diezelfde aanbieders en anderen in en buiten Nederland over dreigingen en incidenten met betrekking tot informatiesystemen (bijvoorbeeld buitenlandse CERT's ten behoeve van de analyse van genoemde dreigingen in relatie tot informatiesystemen van hun eigen doelgroep). Deze taken zijn vastgelegd in artikel 2, eerste lid, onder a en b. Opgemerkt zij hierbij dat de betrokken aanbieders uiteraard zelf primair verantwoordelijk zijn als het gaat om het treffen van maatregelen aangaande de beveiliging van hun informatiesystemen.

Daarnaast heeft het NCSC als taak om analyses en technisch onderzoek te verrichten ten behoeve van de in artikel 2, eerste lid, onderdelen a en b, genoemde taken, naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot vitale informatiesystemen (artikel 2, eerste lid, onder c). Daarbij gaat het met name om het verrichten van analyses op basis van aan het NCSC verstrekte gegevens, teneinde de aard en ernst van dreigingen en incidenten in relatie tot het risico van maatschappelijke ontwrichting te kunnen bepalen en op basis daarvan die aanbieders waarbij een vergelijkbare kwetsbaarheid zich zou kunnen voordoen te kunnen waarschuwen en adviseren. Ook worden technische activiteiten verricht die nodig zijn om die analyses te kunnen verrichten. Denk hierbij bijvoorbeeld aan de situatie waarin het NCSC een gegevensdrager met relevante gegevens over dreigingen en incidenten krijgt aangeleverd en zich eerst in technische zin toegang moet zien te verschaffen tot de inhoud daarvan alvorens de gegevens te kunnen analyseren.[18] Analyses en technisch onderzoek in voornoemde zin door het NCSC geschiedt op basis van gegevens die anderen, zoals vitale aanbieders die incidenten melden of computercrisisteams in andere landen, aan het NCSC verstrekken. Het wetsvoorstel voorziet daarbij in de mogelijkheid om bij andere organisaties informatie op te vragen, zonder dat daarvoor overigens een medewerkingsplicht voor de aangezochte organisatie geldt (artikel 4). Daarbij kan het bijvoorbeeld gaan om de kenmerken van een digitale aanval, om een voorbeeld van aangetroffen malware, om gegevens over de interne verspreiding van malware of om de IP-adressen die daarbij betrokken zijn. Met dergelijke gegevens kan een dreiging of incident worden geanalyseerd en kan aan organisaties worden geadviseerd over beveiliging tegen vergelijkbare digitale aanvallen.
Analyses en technisch onderzoek naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot vitale elektronische informatiesystemen zullen alleen worden uitgevoerd wanneer dit in dienst staat van de NCSC-taken om bijstand te verlenen of te informeren en adviseren. Het NCSC zal daarmee uitdrukkelijk geen onderzoek doen naar personen of organisaties die verantwoordelijk zijn voor die dreigingen en incidenten of daar anderszins aan bijdragen of hebben bijgedragen. Het NCSC is bijvoorbeeld niet bevoegd om de identiteit te achterhalen van diegenen die bewust dan wel (bijvoorbeeld in het kader van een botnet) onbewust een dreiging of incident veroorzaken of veroorzaakt hebben. Dergelijk dadergericht onderzoek is voorbehouden aan de inlichtingen- en veiligheidsdiensten, die daartoe beschikken over wettelijk geregelde

[18] Zie bijv. Kamerstukken II 2012/13, 26 643, nr. 272 (casus Pobelka).

bijzondere inlichtingenmiddelen, en aan de politie en het OM, die daartoe beschikken over opsporingsbevoegdheden. Wel kan het NCSC bijvoorbeeld nagaan of een bij een incident betrokken IP-adres toebehoort aan een vitale aanbieder of aan een andere aanbieder die onderdeel is van de rijksoverheid (op basis van reeds bij het NCSC bekende IP-adressen van die aanbieders), zodat het die aanbieder kan waarschuwen. Het NCSC is echter niet bevoegd om na te gaan welke (natuurlijke) persoon dat IP-adres gebruikt.

Bij het onderzoek naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot informatiesystemen van vitale aanbieders of van niet-vitale aanbieders die onderdeel zijn van de rijksoverheid kunnen ook gegevens aan het licht komen over dreigingen of incidenten met betrekking tot andere informatiesystemen. Denk bijvoorbeeld aan grote hoeveelheden e-mailadressen die door een ICT-inbreuk kwetsbaar zijn geworden of grote hoeveelheden domeinnamen van websites waarop een kwetsbaarheid aanwezig is die gebruikt kan worden om schade toe te brengen aan de bezoeker van die website. Naar mijn oordeel is het niet gewenst als het NCSC in zo'n geval niet bevoegd zou zijn om dergelijke «bijvangst», ter voorkoming van nadelige maatschappelijke gevolgen, te delen met een beperkte kring van derden, bestaande uit:
- organisaties die tot – objectief kenbare – taak hebben om andere organisaties of het publiek over die dreigingen of incidenten te informeren;
- bij ministeriële regeling aangewezen computercrisisteams; en
- aanbieders van internettoegangs- of internetcommunicatiediensten ten behoeve van het informeren van gebruikers van die diensten.[19]

Uit de Wet bescherming persoonsgegevens volgt bovendien dat het NCSC alleen persoonsgegevens verstrekt voor zover dat noodzakelijk is gezien de aard en omvang van de gegevens en de mogelijke maatschappelijke gevolgen daarvan. Het voorgestelde tweede lid van artikel 2, waarin deze gegevensverstrekking als taak is vastgelegd, beoogt het bestaan van de bevoegdheid tot verstrekking van de «bijvangst» buiten twijfel te stellen.

Bij de uitoefening van bovenvermelde taken werkt het NCSC, gezien de raakvlakken met de taakuitoefening van de inlichtingen- en veiligheidsdiensten in het digitale domein, nauw met die diensten samen. In dit verband zij erop gewezen dat de in het onderhavige wetsvoorstel genoemde taken thans reeds door het NCSC worden vervuld, en met dit wetsvoorstel slechts van een steviger wettelijke grondslag worden voorzien. Bij de uitoefening van de taken op het gebied van cybersecurity vindt op verschillende wijzen afstemming plaats en wordt op operationeel, tactisch en strategisch niveau samengewerkt. Voorbeelden daarvan zijn onder meer de reguliere overleggen die door de hoofden van de respectievelijke eenheden worden gehouden teneinde elkaar te informeren over de taakuitoefening van de inlichtingen- en veiligheidsdiensten en het NCSC, de afvaardiging door die diensten van liaisons bij het NCSC, de samenwerking in het kader van onder meer de ondersteuning van organisaties bij het uitvoeren van netwerkdetectie, en het – met inachtneming van de geldende wettelijke kaders – uitwisselen van informatie over onder meer geavanceerde malware. Bij het uitoefenen van de taken door de inlichtingen- en veiligheidsdiensten en het NCSC verschilt het zwaartepunt van de in dat verband te verrichten activiteiten. Voor de inlichtingen- en veiligheidsdiensten ligt de focus op digitale spionage en het voorkomen hiervan alsmede op het achterhalen van de identiteit van actoren. Voor het NCSC geldt dat het zwaartepunt van de activiteiten ligt in het ondersteunen van rijksoverheid en vitale sectoren bij de respons op digitale aanvallen en het duiden van de impact van

[19] Kamerstukken II 2014/15, 26 643, nr. 328 (casus Hold Security).

aanvallen teneinde de weerbaarheid van rijksoverheid en vitale sectoren te verhogen. Middels het voorgaande wordt gezamenlijk bijgedragen aan een algehele verhoging van de veiligheid in het Nederlandse digitale domein.

### 4. Verstrekking van vertrouwelijke gegevens

Het is om twee redenen van groot belang dat de vertrouwelijkheid van bij het NCSC gemelde of anderszins verkregen gegevens over incidenten en kwetsbaarheden betreffende ICT-systemen zo veel mogelijk gewaarborgd is. Ten eerste is dit van belang om te garanderen dat deze gegevens kunnen worden gebruikt door het NCSC voor het uitoefenen van de in artikel 2 van dit wetsvoorstel vermelde taken, zonder daarbij gehinderd te worden door mogelijk vroegtijdig openbaar worden van deze gegevens. Ten tweede is het van belang om schade bij betrokken aanbieders, zoals reputatieschade, benadeling van de concurrentiepositie en toegenomen kwetsbaarheid voor gerichte aanvallen, zo veel mogelijk te voorkomen of te beperken. Wanneer aanbieders terughoudend worden met het delen van vertrouwelijke informatie met het NCSC, benadeelt dat het NCSC in ernstige mate in het goed kunnen uitvoeren van zijn taken. Voor het NCSC, waaraan geen taken betreffende toezicht of handhaving zijn toebedeeld, is het zonder verstrekking, door vitale aanbieders en niet-vitale aanbieders die onderdeel zijn van de rijksoverheid, van gegevens over incidenten en kwetsbaarheden, ook als het meldingen betreft die onverplicht zijn, immers niet goed mogelijk om de rol van kennis- en expertisecentrum te vervullen. Zonder de waarborging van deze functie is het NCSC niet in staat te adviseren en hulp te verlenen bij het verhelpen van incidenten of kwetsbaarheden en zo met name ook de uitval van de beschikbaarheid of betrouwbaarheid van voor de samenleving vitale producten en diensten te voorkomen of te beperken.

Vanwege het bovenstaande bevat het voorgestelde artikel 9 een strikte regeling over het verstrekken, door het NCSC aan derden, van vertrouwelijke gegevens met betrekking tot een aanbieder. Dergelijke gegevens worden slechts aan derden verstrekt (behoudens verplichtingen tot verstrekking uit hoofde van andere wetten en behoudens instemming van de betrokken aanbieder met ruimere verstrekking), als aldaar de geheimhouding van de gegevens in voldoende mate is gewaarborgd en voldoende gewaarborgd is dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt. Voor de verstrekking van vertrouwelijke gegevens die bovendien herleid kunnen worden tot een aanbieder (naam van de aanbieder, etc.) bevat artikel 9 een bijzondere openbaarheidsregeling, die in de plaats treedt van de Wet openbaarheid van bestuur (Wob).[20] Dergelijke gegevens kunnen slechts worden verstrekt aan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) en aan daartoe bij ministeriële regeling aangewezen computercrisisteams, voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer (artikel 9, tweede lid). Daarnaast kan de Staatssecretaris van Veiligheid en Justitie besluiten, wanneer een vitale aanbieder of een niet-vitale aanbieder die onderdeel is van de rijksoverheid onvoldoende gevolg geeft aan een eerder door het NCSC gegeven advies, om dat advies, met inbegrip van de daarin opgenomen herleidbare gegevens, te verstrekken aan andere betrokken bewindspersonen (artikel 9, derde lid). Zie ook de artikelsgewijze toelichting bij artikel 9.

---

[20] Wel blijft de Wob onverkort van toepassing op milieu-informatie, zie de uitzondering in artikel 9, zesde lid, en de toelichting daarbij in het artikelsgewijze deel van deze memorie.

Voorts verstrekt het NCSC herleidbare gegevens aan andere betrokken bewindspersonen wanneer dit noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken (artikel 9, vierde lid, onderdeel a). Daarbij kan bijvoorbeeld worden gedacht aan een dreigende crisissituatie ten aanzien waarvan het nemen van crisisbeheersingsmaatregelen aangewezen kan zijn. Daarbij wordt aangesloten op de bestaande crisisbeheersingsstructuren.

Het voorkomen of beperken van ernstige maatschappelijke gevolgen kán noodzaken tot verstrekking van herleidbare gegevens aan andere organisaties of aan het publiek (artikel 9, vierde lid, onderdeel b). In veel gevallen zal volstaan kunnen worden met niet-herleidbare mededelingen, bijvoorbeeld als het publiek moet worden gewaarschuwd voor de risico's van een door internetcriminelen gehanteerde werkwijze. Soms echter zal de voorlichting alleen effectief kunnen zijn als de aanbieder of het product of de dienst concreet wordt aangeduid, bijvoorbeeld als het nodig is om het publiek te waarschuwen dat er grote risico's verbonden zijn aan het gebruik van een bepaald product of een bepaalde dienst. De beslissing om dergelijke voorlichting te geven, vergt een belangenafweging.[21] Zo zal het belang van het publiek om op de hoogte te zijn niet altijd opwegen tegen het belang van de betrokken aanbieder. Denkbaar is ook dat de bekendmaking de maatschappelijke schade juist veroorzaakt of vergroot in plaats van voorkomt of beperkt. Vandaar mijn voorstel om hiervoor een streng criterium te hanteren: «voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of beperken». Bij «ernstige maatschappelijke gevolgen» moet worden gedacht aan ontwrichting van de Nederlandse samenleving. Het NCSC zal de betrokken organisatie raadplegen bij het maken van bovenvermelde belangenafweging en bij de vorm en inhoud van de concrete publieksmededeling.

Daarnaast ben ik echter ook van mening dat openheid en transparantie van beleid ook in het geval van het NCSC zo veel mogelijk gewaarborgd moeten zijn. Ten aanzien van bij het NCSC berustende gegevens die niet vertrouwelijk zijn, hecht ik daarom bijvoorbeeld aan periodieke publieksmededelingen door het NCSC over bijvoorbeeld voor sectoren geldende aantallen meldingen en typen incidenten. Dergelijke mededelingen beogen de samenleving een beeld te geven van digitale dreigingen en de digitale veiligheid te bevorderen.

Benadrukt zij dat het voorgestelde artikel 9 ziet op alle vertrouwelijke gegevens met betrekking tot aanbieders waarover het NCSC beschikt, en dus niet alleen op vertrouwelijke gegevens die het NCSC heeft verkregen uit verplichte meldingen, maar ook op vertrouwelijke gegevens die zijn verkregen door onverplichte meldingen of naar aanleiding van een verzoek als bedoeld in artikel 4, eigen analyses en technisch onderzoek of mededelingen van derden.

Met bovenstaande regeling wordt naar mijn oordeel voorzien in een goede balans tussen enerzijds het waar nodig ten behoeve van de taakuitoefening van het NCSC, alsook met het oog op belangen van betrokken aanbieders, waarborgen van de vertrouwelijkheid van bij het NCSC berustende informatie over incidenten en kwetsbaarheden, en anderzijds het met inachtneming daarvan zo veel mogelijk kunnen blijven informeren van onder meer het publiek over die incidenten en kwetsbaarheden.

[21] Zie ook artikel 3:4 Algemene wet bestuursrecht (Awb). Deze bepaling geldt in beginsel ook voor andere handelingen – van bestuursorganen – dan besluiten, zie artikel 3:1, tweede lid, Awb.

## 5. Totstandkoming van dit wetsvoorstel[22]

*5.1. Inleiding*

Twee eerdere versies van dit wetsvoorstel zijn opengesteld voor consultatie op www.internetconsultatie.nl[23] en voor commentaar toegezonden aan belangenorganisaties, vitale aanbieders en toezichthoudende organisaties. Gekozen is voor twee consultatierondes omdat het wetsvoorstel bij de eerste consultatie alleen regels bevatte over de meldplicht voor ICT-inbreuken en nadien is uitgebreid met regels over het verwerken van gegevens ten behoeve van de NCSC-taken.
Op het concept voor een «Wet gegevensverwerking en meldplicht cyber security» (voorheen: Wet melding inbreuken elektronische informatiesystemen) is inhoudelijk gereageerd door onder meer VNO-NCW en MKB-Nederland, Nederland ICT, Netbeheer Nederland, Bits of Freedom, Business Communication Providers Alliance (BCPA), Schiphol Group, Vereniging van waterbedrijven in Nederland (Vewin), Nederlandse Vereniging van Banken (NVB), De Nederlandsche Bank (DNB), Autoriteit Financiële Markten (AFM), Eurofiber, T-Mobile, Luchtverkeersleiding Nederland, Euronext, Microsoft, Arthur's Legal, TenneT, Gasunie, Schiphol Group en het College bescherming persoonsgegevens (thans de Autoriteit persoonsgegevens).

*5.2. Bespreking van de reacties op hoofdlijnen*

In totaal hebben twee consultatierondes plaatsgevonden. Hieronder volgt een globale bespreking van de belangrijkste reacties.

5.2.1. Just culture

Er bestaan zorgen omtrent de in de toelichting gepropageerde *just culture*: een veiligheidscultuur waarin het leren van incidenten vooropstaat. Verscheidene partijen vinden dat een wettelijke meldplicht in de weg staat voor het bewerkstelligen van een *just culture.* Een wettelijke meldplicht zou het NCSC een meer toezichthoudende rol geven. **Gasunie** betoogt in dat verband dat een just culture gerealiseerd zou moeten worden op basis van vertrouwelijkheid. **Bits of Freedom** vindt een wettelijke meldplicht juist belangrijk voor het creëren van een *just culture*, en mist in dat kader waarborgen voor naleving van de meldplicht.
**Eurofiber** en **Microsoft** pleiten voor een vrijwillige meldplicht: uitwisseling van informatie op grond van vertrouwen wordt gezien als het belangrijkste element voor het creeren van een *just culture*.
De bestaande meldplicht voor «voorvallen»[24] in de luchtvaart (artikel 7.1 Wet luchtvaart (Wlv)) laat zien dat een wettelijke meldplicht goed te verenigen is met het nastreven van een *just culture,* mits de vertrouwelijkheid van de melding wordt beschermd[25] en de mogelijkheid van het opleggen van sancties naar aanleiding van een gedane melding wordt beperkt.[26] Eerder in deze memorie heb ik uitgelegd waarom ik voorstel om het NCSC niet te belasten met de handhaving van de meldplicht (toezicht en sancties).

---

[22] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer
[23] Zie www.internetconsultatie.nl/meldplicht_ict_inbreuken en www.internetconsultatie.nl/cybersecurity.
[24] Een voorval is een operationele onderbreking, defect, fout of andere onregelmatigheid, waardoor de vliegveiligheid wordt of kan worden beïnvloed, zonder dat sprake is van een ongeval of ernstig incident (artikel 1.1 Wlv).
[25] Zie artikel 7.2 Wlv en artikel 4, tweede lid, Regeling melding voorvallen in de burgerluchtvaart.
[26] Zie de artikelen 11.25 en 11.26 Wlv.

5.2.2. Zorgplichten en handhaving

Daarnaast pleiten twee inzenders, in het licht van handhaving door het NCSC, voor de inzet (al dan niet verplicht) van «intrusion detection software», programmatuur die ICT-inbreuken detecteert.
Het NCSC kan in een concreet geval adviseren om programmatuur zoals de in twee van de inzendingen genoemde «intrusion detection software» te installeren. In het licht van de publiek-private samenwerking voorziet dit wetsvoorstel niet in interventiebevoegdheden zoals een organisatie verplichten tot het nemen van een bepaalde beveiligingsmaatregel. Wel heb ik mede naar aanleiding van de hier besproken consultatiereacties het wetsvoorstel op enkele punten aangepast (zie ook paragraaf 5.2.7. Vertrouwelijkheid):

5.2.3. Reikwijdte meldplicht

In veel reacties zijn vragen gesteld over de reikwijdte van de meldplicht. Zo was voor verschillende partijen onduidelijk voor welke vitale aanbieders, producten en diensten de meldplicht zal gelden en wanneer is voldaan aan het criterium «in belangrijke mate» van artikel 6. Daarnaast vindt een inzender dat de meldplicht ook voor de gezondheidszorg moet gaan gelden, wordt gevraagd welke juridische kaders er bestaan voor de aanwijzing van vitale aanbieders en vindt een inzender de meldplicht onnodig specifiek: elke situatie die cruciale dienstverlening in gevaar brengt moet volgens deze inzender onder de meldplicht vallen.
**Gasunie** betoogt daarentegen dat de meldplicht alleen moet gelden voor incidenten met grote maatschappelijke en economische gevolgen en ziet dit graag uitgewerkt in algemene maatregelen van bestuur (amvb's).
**BCPA, VNO-NCW** en **Microsoft** vinden de formulering van de reikwijdte van de meldplicht in het wetsvoorstel nog te onduidelijk en één inzender noemt de formulering nog te breed.
Om de meldplicht nader in te vullen, is en wordt de wenselijke reikwijdte van de meldplicht besproken met betrokken partijen uit de vitale sectoren. Vervolgens zullen de (categorieën van) vitale aanbieders, producten en diensten die onder de meldplicht gaan vallen, worden aangewezen bij amvb.
Het overleg met de vitale sectoren dient ook om te bespreken wat voor de verschillende producten en diensten moet worden verstaan onder «in belangrijke mate». Het is de bedoeling om dat in te vullen met een goed hanteerbaar, objectief criterium. Dit leidt per sector of onderdeel van een sector tot een specifieke uitwerking, die in overleg met de sector plaatsvindt. Alleen producten en diensten waarvan de beschikbaarheid en betrouwbaarheid van vitaal belang zijn voor de Nederlandse maatschappij vallen onder de meldplicht. De gezondheidszorg wordt niet als «randvoorwaardelijke» vitale sector bestempeld, vanwege het geringere risico van cascade-effecten, en geldt daarom niet als vitaal in de zin van artikel 1 van het wetsvoorstel. Daarnaast valt een uitbreiding van de meldplicht naar elke situatie die cruciale dienstverlening in gevaar brengt buiten de reikwijdte van de taken, expertise en kennis van het NCSC, daar er voor betrokkenheid van het NCSC sprake moet zijn van een digitale component (een ICT-inbreuk).
Verder is in artikel 1 van het wetsvoorstel in de definitie van aanbieder «degene die» vervangen door «overheidsorganisatie of privaatrechtelijke rechtspersoon die» en is in artikel 5 naar aanleiding van meerdere reacties toegevoegd dat de aanwijzing bij amvb van de onder de meldplicht vallende vitale aanbieders, producten en diensten de vorm mag krijgen van aan te wijzen *categorieën*. In artikel 7, sub b (a oud), is verduidelijkt dat de bepaling niet alleen ziet op de risico's voor aangewezen producten of diensten, maar op alle risico's voor de informatiesystemen van de

doelgroep van het NCSC: vitale aanbieders en niet-vitale aanbieders die onderdeel zijn van de rijksoverheid.

5.2.4. Te melden ICT-inbreuken

Door onder meer **Microsoft** is betoogd dat de te melden ICT-inbreuken duidelijk en precies geformuleerd moeten worden. Dit gebeurt volgens deze partijen nu onvoldoende. **LVNL** noemt de invulling per amvb van de termen «in belangrijke mate» en «producten en diensten» van essentieel belang. **NVB/BVN** geeft aan het wenselijk te vinden de meldplicht slechts bij daadwerkelijke maatschappelijk ontwrichting voor te schrijven en is van mening dat de wet teveel ruimte laat om sectoren bij kleine incidenten te bevragen. **Bits of Freedom** betoogt daarnaast dat DDoS-aanvallen die wel tot maatschappelijke ontwrichting kunnen leiden ook onder de meldplicht zouden moeten vallen.
Zoals eerder in deze toelichting aangegeven, zal de vaststelling van de organisaties, producten en diensten die onder de meldplicht vallen geschieden bij amvb. Het begrip «in belangrijke mate», dat leidend is voor de vaststelling of een ICT-inbreuk onder de meldplicht valt, zal per sector worden geconcretiseerd en die invulling kan bijvoorbeeld worden vastgelegd in richtsnoeren of bij of krachtens de in artikel 8 bedoelde amvb.

5.2.5. Administratieve lasten

In diverse reacties (onder andere van **Eurofiber, BCPA, T-Mobile, Euronext, NVB/BVN** en **Gasunie**) wordt bezorgdheid uitgesproken over de administratieve lasten door het bestaan van deels overlappende verplichtingen tot melding van incidenten bij meerdere instanties. De voorgestelde extra meldplicht wordt gezien als lastenverhogend, ondoelmatig, onduidelijk en ineffectief, wat kan leiden tot vertraging bij het oplossen van een ICT-inbreuk. **NVB/BVN** pleit voor een efficiënte kosten/batenafweging bij het vaststellen van de informatiebehoefte van het NCSC.
In de memorie van toelichting is naar aanleiding van de reacties van de **NVB/BVN** en **VNO-NCW** verduidelijkt waarom de administratieve lasten voor aanbieders die onder de meldplicht komen te vallen naar verwachting beperkt zullen blijven. Daarnaast is in de memorie van toelichting toegelicht dat de meldplicht ook tot doel heeft te voorkomen dat grote ICT-inbreuken die de beschikbaarheid of betrouwbaarheid van een voor de Nederlandse samenleving vitaal product of vitale dienst in belangrijke mate kunnen onderbreken, niet of niet tijdig worden gemeld, of dat getrapte melding hierin te veel vertraging zou kunnen opleveren. Ik heb een eigen verantwoordelijkheid op het gebied van cybersecurity. Met behulp van de meldplicht word ik in staat gesteld aan deze verantwoordelijkheid te voldoen.

5.2.6. Verhouding tot NIB-richtlijn

**VNO-NCW**, **MKB-Nederland**, **BCPA** en **Nederland ICT** pleiten voor uitstel van de meldplicht totdat de tekst van de NIB-richtlijn vaststaat, om te voorkomen dat de nu voorgestelde meldplicht al na korte tijd moet worden gewijzigd.

Naar aanleiding van deze opmerkingen ben ik in paragraaf 2.7 en 2.9 uitgebreider ingegaan op de keuze om een wettelijke meldplicht te introduceren vooruitlopend op de implementatie van de NIB-richtlijn.

5.2.7. Vertrouwelijkheid

Verder bestaan zorgen omtrent de vertrouwelijkheid van de zich bij het NCSC bevindende gegevens. **DNB** en **AFM** pleiten bijvoorbeeld voor beperking van de bevoegdheid van het NCSC om gevoelige gegevens aan derden te verstrekken. Verder pleiten partijen ervoor gevoelige gegevens niet aan derden te verstrekken zonder instemming van (**NVB**) dan wel overleg met (**Nederland ICT**) de betrokken vitale aanbieder. **DNB** en **AFM** betogen dat sectorale toezichthouders moeten beslissen over verstrekking van dergelijke gegevens aan derden.

In het voorgestelde artikel 9, dat in de plaats is gekomen van artikel 6 uit de eerste consultatieversie, is aan deze zorgen gehoor gegeven. Zie paragraaf 4 en de artikelsgewijze toelichting bij artikel 9. Een en ander leidt ertoe dat voor het NCSC inderdaad, zoals **DNB en AFM** bepleiten, een geheimhoudingsplicht gaat gelden die vergelijkbaar is met de geheimhoudingsplicht van (deze)[27] sectorale toezichthouders. En doordat artikel 9 zich beperkt tot vertrouwelijke bedrijfsgegevens, is duidelijker dan bij artikel 6 (oud) dat artikel 9 niet in de weg staat aan actieve openbaarmaking van bijvoorbeeld aantallen meldingen en typen incidenten, zoals bepleit door **Bits of Freedom**.

Verder is in artikel 9 de drempel voor een verstrekking van herleidbare gegevens aan andere organisaties of het publiek verhoogd naar: «voor zover dat noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken» (vierde lid). Dit criterium geldt ook voor verstrekking aan derden van vertrouwelijke herleidbare gegevens over incidenten en kwetsbaarheden die niet onder de meldplicht vallen. Als voldaan is aan dit criterium, dus als verstrekking van vertrouwelijke herleidbare gegevens inderdaad noodzakelijk is om ernstige maatschappelijke gevolgen te voorkomen of te beperken, dan zou het onjuist zijn als een afzonderlijke aanbieder de verstrekking niettemin zou kunnen tegenhouden. Ook een vetorecht van een toezichthouder zou in dat geval geen recht doen aan de eigen verantwoordelijkheid en expertise van het NCSC. Intussen zal het NCSC de betrokken aanbieder (tenzij de gegevens worden verstrekt aan een andere bewindspersoon, artikel 9, vierde lid, onder a) en zo mogelijk ook de toezichthouder wel raadplegen over de voorgenomen verstrekking, teneinde de nodige kennis te vergaren over de relevante feiten en de af te wegen belangen.[28]
De **Schiphol Group** heeft gevraagd of het NCSC zelf bepaalt dat aan het publiek mededelingen mogen worden gedaan over vertrouwelijke herleidbare gegevens (artikel 9, vierde lid, onder b). Het NCSC voert zijn taken in beginsel zelfstandig uit krachtens mandaat, volmacht en machtiging. Het is dus in beginsel aan het NCSC om de in artikel 9 gehanteerde criteria uit te leggen. Wel zal de Staatssecretaris van Veiligheid en Justitie zelf beslissen over het al dan niet toezenden van een NCSC-advies (uiteraard inclusief herleidbare gegevens) aan een andere bewindspersoon indien de betrokken vitale aanbieder onvoldoende gevolg geeft aan het advies. Het NCSC zal dus niet zelf beslissen over de toepassing van het derde lid van artikel 9.
Ten slotte stelden **T-Mobile** en **NVB/BVN** vragen over de reikwijdte van artikel 9, zesde lid. De voorgestelde tekst bepaalt expliciet dat de Wob niet van toepassing is op vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder (behoudens milieu-informatie). Deze uitzondering geldt voor alle herleidbare gegevens die zich bij het NCSC bevinden, dus zowel

[27] Zie de artikelen 1:89 tot en met 1:93c van de Wet op het financieel toezicht.
[28] Vgl. artikel 3:2 Awb: «Bij de voorbereiding van een besluit vergaart het bestuursorgaan de nodige kennis omtrent de relevante feiten en de af te wegen belangen». Deze bepaling geldt in beginsel ook voor andere handelingen dan besluiten, zie artikel 3:1, tweede lid, Awb.

voor gegevens die het NCSC op grond van de meldplicht, als op grond van vrijwillige meldingen heeft ontvangen. De uitzondering geldt niet alleen zolang die gegevens bij het NCSC berusten, maar ook nadat zij, na verstrekking door het NCSC op grond van artikel 9, bij een ander overheidsorgaan berusten.

5.2.8. Behandeling van de melding door het NCSC

Een aantal indieners vragen of de behandeling van de meldplicht door het NCSC inzichtelijk gemaakt kan worden en hoe met informatie die het NCSC op grond van deze melding heeft verkregen wordt omgegaan.
In deze memorie is verduidelijkt hoe een melding door het NCSC in behandeling zal worden genomen (**Eurofiber**). Naar aanleiding van de reactie van **Arthur's Legal** op artikel 3 van het wetsvoorstel is in de memorie de opmerking toegevoegd dat bedrijfsvertrouwelijke gegevens die niet (langer) noodzakelijk zijn voor het uitvoeren van de taken van het NCSC zullen worden vernietigd. Voor persoonsgegevens geldt deze eis al op grond van de Wet bescherming persoonsgegevens.

5.2.9. Advies van de Autoriteit persoonsgegevens

1. De Autoriteit persoonsgegevens (AP) vindt de grondrechtentoets onvoldoende onderbouwd en is van mening dat het voorstel, gelet op de (mogelijke) verwerking van bijzondere persoonsgegevens in de zin van artikel 16 Wbp en de afwijking van artikel 9 Wbp in artikel 4 van dit wetsvoorstel, onvoldoende passende waarborgen bevat.
   Naar aanleiding van het AP-advies is in par. 6 (eerste alinea) van deze memorie ingegaan op de situatie dat een organisatie aan het NCSC een dataset wil geven waarin (mogelijk ook) bijzondere persoonsgegevens zitten. Zie voor artikel 9 Wbp hierna.
2. De AP vindt de reikwijdte van het voorstel onduidelijk, vanwege niet of onvoldoende omschreven begrippen zoals *vertrouwelijke gegevens, vitaal belang, vitale aanbieder, onverwijld kennis [geven]* en *in belangrijke mate;* bovendien is (een deel van) de groep van ontvangers van de gegevens onbepaald (artikel 2, tweede lid, onderdeel a).
   Het begrip *vertrouwelijke gegevens* wordt alleen gebruikt in artikel 9, eerste lid. Het ziet daar op gegevens met betrekking tot *aanbieders* (in de zin van dit wetsvoorstel, zie de definitie in artikel 1). Naar aanleiding van het AP-advies is dat ook in de bepaling zelf tot uitdrukking gebracht en is de toelichting bij artikel 9 aangevuld.
   Het begrip *vitaal belang* wordt alleen gebruikt in de definitie van *vitale aanbieder*. Ter verduidelijking van *vitale aanbieder*, en daarmee ook van *vitaal belang*, is in de toelichting bij artikel 1 een verwijzing opgenomen naar de «Herijkte lijst vitale infrastructuur».
   De term *onverwijld* in artikel 6, eerste lid, wordt al voldoende toegelicht in par. 2.2 en in de toelichting bij artikel 6. Wat in een concreet geval *onverwijld* is, hangt af van de omstandigheden.
   Ook het begrip *in belangrijke mate* is al voldoende toegelicht (par. 2.4 en toelichting bij artikel 6).
   In artikel 2, tweede lid, onderdeel a, is toegevoegd dat de daar bedoelde taak *objectief kenbaar* moet zijn, ter verduidelijking van de groep waaraan zogeheten «bijvangst» kan worden doorverstrekt.
3. De AP vindt de afwijking van artikel 9 Wbp onvoldoende onderbouwd. Die bepaling verbiedt «verdere» verwerking van persoonsgegevens op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (eerste lid), en stelt buiten twijfel dat het verder verwerken van persoonsgegevens hoe dan ook verboden is als ingevolge ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt (vierde lid). Wat betreft het eerste lid wijst de AP erop dat artikel 43 Wbp al

voorziet in een mogelijkheid om het doelbindingsbeginsel buiten toepassing te laten.
Naar aanleiding van het AP-advies is de afwijking van artikel 9 beperkt tot het doelbindingsbeginsel (eerste lid). De afwijking van de geheimhoudingsplicht (vierde lid) is geschrapt, omdat zij bij nader inzien inderdaad niet nodig is. Verder is aan de toelichting bij artikel 4 een passage toegevoegd waarin wordt uitgelegd waarom artikel 43 Wbp geen soelaas biedt wat betreft het eerste lid van artikel 9 Wbp.

4. Reagerend op een passage in par. 2.6 van de toelichting merkt de AP op dat het zeer de vraag is of kan worden voorkomen dat de mogelijke samenloop van de meldplicht voor ICT-inbreuken en de meldplicht datalekken voor bedrijven tot meer administratieve lasten leidt.
Naar aanleiding van deze opmerking is de passage geschrapt.

5.3.10. Diversen

Naar aanleiding van allerlei specifieke vragen en opmerkingen zijn het wetsvoorstel en de memorie van toelichting op verschillende plaatsen gewijzigd of aangevuld. Zo is toegelicht wat moet worden verstaan onder de term hersteltijd van artikel 6, tweede lid, onder d, van het wetsvoorstel. Verder is naar aanleiding van een reactie van **Euronext** in de wettekst bij artikel 6, tweede lid, het «tijdstip van aanvang van de ICT-inbreuk» afgezwakt tot «vermoedelijke tijdstip». In de memorie van toelichting is ook de verhouding tussen artikel 4 en artikel 9 beter toegelicht.

## 6. Grondrechtentoets

Het NCSC krijgt vanuit zijn rol als informatieknooppunt in het nationale en internationale netwerk met regelmaat de beschikking over aanzienlijke hoeveelheden data. Deze data komen binnen in het kader van een signalering van een incident of dreiging met betrekking tot een elektronisch informatiesysteem waarbij Nederlandse vitale aanbieders of niet-vitale aanbieders die onderdeel zijn van de rijksoverheid betrokken kunnen zijn. Dit wetsvoorstel voorziet in een bevoegdheid om deze gegevens te verkrijgen en verder te verwerken ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van dergelijke elektronische informatiesystemen en ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving. Vaak bevat een dataset IP-adressen, e-mailadressen en domeinnamen. Daarnaast verwerkt het NCSC contactgegevens van medewerkers van aanbieders die voor het NCSC als contactpersoon fungeren en van andere melders van incidenten en kwetsbaarheden. Het is denkbaar dat aan het NCSC een dataset wordt aangeboden die ook bijzondere persoonsgegevens bevat. Vooropgesteld zij dat het voor het NCSC met het oog op de uitoefening van de in artikel 2 van dit wetsvoorstel bedoelde taken niet nodig is om over bijzondere persoonsgegevens te beschikken. Uitgangspunt is dan ook dat het NCSC geen datasets in ontvangst neemt waarvan bekend is of vermoed wordt dat daarin ook bijzondere persoonsgegevens voorkomen. Degene die een dataset aanbiedt zal in een dergelijk geval worden gevraagd om de dataset te filteren en alleen die gegevens aan het NCSC te verstrekken die noodzakelijk zijn voor het uitvoeren van de NCSC-taken.[29] Voor bijvoorbeeld vitale aanbieders die het NCSC gegevens over dreigingen of incidenten willen verstrekken, geldt overigens uiteraard dat zij ook zelf, zeker ook aangaande bijzondere persoonsgegevens die mogelijkerwijs deel uitmaken van een dataset, de Wbp in acht moeten nemen. Mocht pas na

[29] Zie bijvoorbeeld ook de Hold Security-casus, waar door het NCSC is verzocht slechts dat deel van de beschikbare data aan te leveren dat noodzakelijk was voor de uitvoering van de taken van het NCSC.

ontvangst van een dataset blijken dat daarin toch bijzondere persoonsgegevens voorkomen, dan zullen deze door het NCSC onmiddellijk worden vernietigd.

De verwerking van persoonsgegevens door het NCSC is een inmenging door het openbaar gezag in het recht op respect voor de persoonlijke levenssfeer (de artikelen 10 Grondwet, 8 EVRM[30] en 17 IVBPR[31]). Artikel 8, eerste lid, EVRM bepaalt dat een ieder recht heeft op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Het tweede lid staat inmenging in dit recht op respect voor de persoonlijke levenssfeer alleen toe voor zover zij bij wet is voorzien, een geoorloofd, expliciet genoemd doel dient en noodzakelijk is in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) nader ingevuld met de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit. Het wetsvoorstel is aan deze beginselen getoetst. Die toetsing wordt hieronder besproken. Het wetsvoorstel is ook getoetst aan artikel 10 Grondwet en artikel 17 IVBPR. Die toetsing leidt niet tot andere gezichtspunten.

*1. De beperkende maatregel moet «voorzien bij wet» zijn*

De voorgestelde artikelen 2 en 3 bieden een specifieke wettelijke grondslag voor de verwerking van persoonsgegevens door het NCSC. Artikel 3 beperkt de verwerking van (persoons)gegevens tot de in artikel 2 omschreven doeleinden en taken. Voor een bespreking van de in artikel 2 omschreven taken zij verwezen naar paragraaf 3. Specifiek wat betreft de onderzoekstaak (artikel 2, eerste lid, onder c) zij er ook hier op gewezen dat analyses en technisch onderzoek naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot vitale elektronische informatiesystemen alleen tot de NCSC-taken behoort als het in dienst staat van de NCSC-taken om bijstand te verlenen of te informeren en adviseren. Het is derhalve geen NCSC-taak om onderzoek te doen naar personen of organisaties die verantwoordelijk zijn voor die dreigingen en incidenten. Dergelijk onderzoek is voorbehouden aan de inlichtingen- en veiligheidsdiensten, die daartoe beschikken over wettelijk geregelde bijzondere inlichtingenmiddelen, en aan de politie en het OM, die daartoe beschikken over opsporingsbevoegdheden.

*2. De beperking moet een legitiem doel dienen en noodzakelijk zijn*

Artikel 8, tweede lid, EVRM, bepaalt dat inmenging in het recht op respect voor het privéleven uitsluitend is toegestaan binnen de kaders van de expliciet en limitatief in dat lid opgesomde belangen. Voor de verwerking van persoonsgegevens door het NCSC geldt dat deze primair plaatsvindt teneinde de beschikbaarheid en de integriteit van informatiesystemen die nodig zijn ten behoeve van overheidsdiensten en andere voor de samenleving vitale producten en diensten, te waarborgen, en zodoende maatschappelijke ontwrichting te voorkomen. Deze verwerking dient onder meer de nationale veiligheid, de openbare veiligheid en het economisch welzijn van het land. Deze belangen staan genoemd in artikel 8, tweede lid, EVRM.

De beperking dient bovendien noodzakelijk te zijn in een democratische samenleving. Het noodzaakcriterium wordt in de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) nader ingevuld met

---

[30] Europees Verdrag tot bescherming van de Rechten van de Mens en de fundamentele vrijheden.

[31] Internationaal Verdrag inzake burgerrechten en politieke rechten.

de vereisten van een dringende maatschappelijke behoefte, proportionaliteit en subsidiariteit. Staten moeten redenen aandragen die voldoende en relevant zijn en hebben daarbij een eigen beoordelingsruimte.

*2a. Dringende maatschappelijke behoefte*

De dringende maatschappelijke behoefte van de verwerking van persoonsgegevens door het NCSC is gelegen in de grote afhankelijkheid van de samenleving van elektronische informatiesystemen, die bovendien onderling verweven zijn. De zorg voor veiligheid is een kerntaak van de overheid. Waarborging van de beschikbaarheid en betrouwbaarheid van diensten en producten van vitale aanbieders en andere van de rijksoverheid deel uitmakende aanbieders is dan ook belangrijk om maatschappelijke ontwrichting te voorkomen. IP-adressen worden door het NCSC verwerkt om de aard en ernst van digitale dreigingen en incidenten te kunnen beoordelen en om derden, met name vitale aanbieders en andere van de rijksoverheid deel uitmakende aanbieders, te kunnen waarschuwen en bijstaan. Enerzijds onderzoekt het NCSC de gegevens die deel uitmaken van een incidentmelding om te achterhalen vanaf welke IP-adressen een digitale aanval wordt uitgevoerd. Die IP-adressen worden verstrekt aan derden (binnen de kaders van de artikelen 2 en 9) om hen in staat te stellen maatregelen te nemen tegen (mogelijke) aanvallen vanaf die adressen. Anderzijds onderzoekt het NCSC of de bij het NCSC bekende IP-adressen van vitale aanbieders en andere tot de rijksoverheid behorende aanbieders getroffen of kwetsbaar zijn en waarschuwt zo nodig de betrokken organisaties.
E-mailadressen worden door het NCSC verwerkt om derden te kunnen waarschuwen. Zo kan het voorkomen dat een door het NCSC ontvangen dataset e-mailadressen bevat die zijn buitgemaakt bij een ICT-inbreuk. Deze e-mailadressen kunnen voor malafide doeleinden gebruikt worden, zoals het versturen van spam, of kunnen – doordat zij betrokken zijn bij een ICT-inbreuk – een kwetsbaarheid vormen voor de organisatie waartoe zij behoren. Ook hierover informeert het NCSC derden binnen de kaders van de artikelen 2 en 9 opdat zij maatregelen kunnen nemen om de beschikbaarheid of betrouwbaarheid van hun informatiesystemen te waarborgen. Verder verwerkt het NCSC de e-mailadressen van melders en andere contactpersonen van onder meer aanbieders van producten en diensten. Deze informatie is noodzakelijk om gevolg te kunnen geven aan een melding, het waarschuwen van anderszins gebleken betrokkenheid bij een ICT-inbreuk, of het informeren en adviseren over gebleken digitale dreigingen of kwetsbaarheden.
Domeinnamen worden door het NCSC verwerkt als het NCSC bij een melding informatie krijgt over kwetsbaarheden in websites. Om de digitale weerbaarheid van de Nederlandse samenleving te verhogen en nadelige maatschappelijke gevolgen te beperken of voorkomen is het van belang dat het NCSC ook deze informatie kan analyseren en (binnen de kaders van de artikelen 2 en 9) kan delen met de juiste organisaties.

*2b. Proportionaliteit*

Het NCSC verwerkt grote aantallen persoonsgegevens,[32] maar gelet op de aard ervan (bv. IP- en e-mailadressen, contactgegevens van melders), het doel waarvoor zij worden verwerkt en de overige waarborgen waarmee deze gegevens zijn omkleed, gaat het niet om een forse inmenging in het recht op respect voor iemands privéleven. Zo doet het NCSC geen onderzoek naar individuele personen die bij een ICT-inbreuk betrokken zijn. De betrokken gegevens worden door het NCSC verwerkt met

---

[32] Zie bijvoorbeeld de getallen, genoemd in de brief van 13 oktober 2014, Kamerstukken II 2014/15, 26 643, nr. 328 (casus Hold Security).

inachtneming van de Wet bescherming persoonsgegevens, onder intern toezicht van de functionaris gegevensbescherming en onder extern toezicht van de Autoriteit persoonsgegevens. Het NCSC verwerkt slechts gegevens voor zover dat noodzakelijk is voor het uitvoeren van de in artikel 2 genoemde taken. Persoonsgegevens die het NCSC verwerkt ten behoeve van zijn taken worden bovendien niet langer door het NCSC bewaard dan noodzakelijk. Zo worden contactgegevens van de melder bijvoorbeeld na maximaal 13 maanden na het afhandelen van de melding vernietigd en worden andere persoonsgegevens, die benodigd zijn voor de uitoefening van de taken van het NCSC, uiterlijk 18 maanden na het afhandelen van een incident of dreiging vernietigd. Deze bewaartermijnen zijn gebaseerd op de blijkens de huidige NCSC-praktijk gemiddeld benodigde maximale termijn om de NCSC-taken naar behoren te kunnen vervullen. Zo moet ook na enige tijd nog contact kunnen worden gezocht met de melder, bijvoorbeeld voor opvolging (hoe staat het er nu voor? heeft de aanbieder het NCSC-advies gevolgd of zijn er andere maatregelen getroffen?) of om hem te waarschuwen voor kwetsbaarheden die zijn systeem opnieuw in gevaar kunnen brengen. Andere persoonsgegevens in voormelde zin (bv. IP-adressen) kunnen van belang zijn als bijvoorbeeld blijkt dat een bepaald IP-adres opnieuw geraakt wordt of een digitale aanval steeds vanuit dezelfde hoek komt. Dit kan voor het NCSC aanleiding zijn om te onderzoeken of de aanval ook relevant is voor andere recent getroffen IP-adressen. Ook kan uit nieuw onderzoek van een afgehandeld incident blijken dat relevante informatie, zoals een kwetsbaarheid van bepaalde IP-adressen of een bepaalde aanvalstechniek, over het hoofd is gezien.
De bewaartermijnen zullen geregeld opnieuw worden beoordeeld en zullen dan zo mogelijk worden verkort en zo nodig worden verlengd. De huidige door het NCSC gehanteerde bewaartermijnen komen overigens overeen met de internationaal door CERT's gehanteerde termijnen.

*2c. Subsidiariteit*

Het NCSC kan zijn taken niet uitoefenen wanneer het niet zou beschikken over de persoonsgegevens die vaak deel uitmaken van datasets die het NCSC verkrijgt bij de melding van een incident. Het NCSC kan niet op andere wijze de informatie verkrijgen die noodzakelijk is voor het uitoefenen van zijn taken. Ook anonimiseren of pseudonimiseren[33] van de data is voor het NCSC niet mogelijk: als de data niet individualiseerbaar zijn, dan kan het NCSC niet onderzoeken welke partijen zijn geraakt en hen rechtstreeks informeren en dan kan het ook de herkomst en het verdere verloop van de dreiging of het incident niet onderzoeken.

*3. Conclusie*

De verwerking van persoonsgegevens door het NCSC is een gerechtvaardigde beperking van de persoonlijke levenssfeer met het oog op het waarborgen van de digitale veiligheid. De voorgestelde bevoegdheden zijn omkleed met voldoende waarborgen, zoals hierboven is uiteengezet.

## 7. Privacy impact assessment

Gezien de aard van dit wetsvoorstel is in de fase van beleidsontwikkeling een Privacy Impact Assessment uitgevoerd.[34] Met behulp hiervan is de noodzaak van de gegevensverwerking bekeken, en zijn op gestructureerde wijze de implicaties in kaart gebracht. Hierbij is in het bijzonder aandacht

---

[33] Het vervangen, met een bepaald algoritme, van identificerende gegevens door versleutelde gegevens.

[34] Zie Toetsmodel Privacy Impact Assessment Rijksdienst, Kamerstukken I 2012/13, 31 051, F.

besteed aan de beginselen van gegevensminimalisering en doelbinding, het vereiste van een goede beveiliging en de rechten van de betrokkenen. De gezichtspunten die relevant zijn voor de eerste twee beginselen zijn voldoende aan de orde gekomen in paragraaf 6.

*Beveiliging*

Voor het NCSC staat het waarborgen van de kwaliteit en veiligheid van gegevens voorop. Zo neemt het NCSC uitvoerige maatregelen om de gegevens te beveiligen die zijn opgeslagen op zijn servers. Verder vindt strikte fysieke en digitale toegangscontrole plaats, waarmee toegang door onbevoegden of verlies van de gegevens zo veel mogelijk wordt beperkt.

*Rechten betrokkene*

Wanneer een betrokkene inzicht wil verkrijgen in de persoonsgegevens die het NCSC over hem of haar verwerkt, deze gegevens wil wijzigen of aanpassen, kan de betrokkene hiertoe een verzoek indienen bij het Ministerie van Veiligheid en Justitie. De gegevens worden vernietigd zodra deze niet langer noodzakelijk zijn voor het verwezenlijken van het doel van de verwerking.

Voor de verwerking van persoonsgegevens door het NCSC is de Staatssecretaris van Veiligheid en Justitie verantwoordelijk. De Autoriteit persoonsgegevens en de functionaris voor de gegevensbescherming van het ministerie houden toezicht op de verwerking van persoonsgegevens door het NCSC.

## 8. Regeldruk

De door dit wetsvoorstel veroorzaakte regeldruk bestaat uit een bescheiden stijging van de administratieve lasten voor de organisaties die onder de meldplicht vallen. Een definitieve raming kan met name pas worden gemaakt als vaststaat voor welke vitale aanbieders en voor welke producten en diensten de meldplicht zal gelden (krachtens artikel 5 aan te wijzen bij amvb). In de nota van toelichting bij deze amvb (en in de toelichting bij de krachtens artikel 8 eventueel vast te stellen nadere regels) zal hierop nader worden ingegaan. Bovendien ben ik voornemens om samen met de betrokken sectoren en departementen nader uit te werken, zo mogelijk per sector, bijvoorbeeld bij of krachtens algemene maatregel van bestuur of in richtsnoeren, welke inbreuken ernstig genoeg zijn om onder de meldplicht te vallen (nadere uitwerking van «in belangrijke mate» in artikel 6, eerste lid). Ook die nadere uitwerking bepaalt voor een deel de omvang van de administratieve lasten.

Intussen mag wellicht een eerste indicatie van de te verwachten administratieve lasten worden ontleend aan de hierboven al besproken meldplicht voor de aanbieder van een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst (artikel 11a.2 Telecommunicatiewet). De totale administratieve lasten van die meldplicht zijn destijds geraamd op circa € 17.000 per jaar, uitgaande van acht aanbieders met elk tien meldingen per jaar. Het daadwerkelijke aantal door het Agentschap Telecom ontvangen meldingen in de afgelopen jaren was ongeveer de helft. Zo waren er 38 meldingen in 2013 en 41 in 2014. Dit betekent overigens niet automatisch een halvering van de destijds geraamde administratieve lasten: naast het doen van de melding vindt er regelmatig nog nader contact plaats met de aanbieder over de verdere details van het incident. Hoewel de in dit wetsvoorstel geregelde meldplicht voor ICT-inbreuken zal gaan gelden voor een groter aantal aanbieders dan waarvan voor artikel 11a.2 Telecommunicatiewet is

uitgegaan, zal het ook bij de onderhavige meldplicht niet gaan om een groot aantal meldingen, daar alleen die inbreuken dienen te worden gemeld waarbij sprake is van een belangrijke onderbreking of belangrijke potentiële onderbreking van de beschikbaarheid of betrouwbaarheid van de vitale dienst of het vitale product.

Zoals gezegd zullen voor elkaar overlappende meldplichten de wijze waarop moet worden gemeld en de gegevens die dienen te worden verstrekt, zo veel mogelijk onderling worden afgestemd.

Voor het overige heeft dit wetsvoorstel geen gevolgen voor de regeldruk voor burgers of het bedrijfsleven.

## Artikelsgewijze toelichting

### Artikel 1

De omschrijving van «aanbieder» is (afgezien van het element «bouwen») afgeleid van de definitie van «aanbieden» in artikel 1.1, onder i, van de Telecommunicatiewet. Het begrip slaat zowel op privaatrechtelijke rechtspersonen als op overheidsorganisaties (al dan niet onderdeel van de rijksoverheid).

Het begrip «vitale aanbieder» slaat alleen op aanbieders van voor de Nederlandse samenleving vitale producten of diensten. Daaronder worden de aanbieders verstaan die producten of diensten leveren die behoren bij de vitale processen, genoemd in de «Herijkte lijst vitale infrastructuur», zoals deze in mei 2015 is aangeboden aan de Tweede Kamer en in 2015 op onderdelen nog zal worden aangevuld.[35] De meldplicht kan alleen gelden voor vitale aanbieders (zie artikel 5), maar hoeft niet per se voor alle vitale aanbieders te gelden.

Bij informatiesystemen zal het vaak gaan om systemen die van internet afhankelijk zijn, maar dat is geen vereiste.

De begrippen persoonsgegevens, verwerking van persoonsgegevens en verantwoordelijke hebben dezelfde betekenis als in de Wet bescherming persoonsgegevens (Wbp). Onder persoonsgegevens verstaat artikel 1 Wbp «elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon». In het kader van dit wetsvoorstel betreft het bij de verwerking van persoonsgegevens door het NCSC, zoals hierboven is aangegeven, bijvoorbeeld bij incidenten of dreigingen betrokken IP-adressen (nummers waarmee een individuele computer, en daarmee vaak ook de gebruiker daarvan, geïdentificeerd kan worden) en contactgegevens van bijvoorbeeld overheids- en vitale private partijen. Zie ook artikel 3.

Onder verwerking van persoonsgegevens verstaat de Wbp «elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens».

---

[35] Kamerstukken II 2014/15, 30 821, nr. 23, p. 5.

Onder verantwoordelijke verstaat de Wbp «de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt». In het kader van dit wetsvoorstel gaat het om de Staatssecretaris van Veiligheid en Justitie.

**Artikel 2**

Dit artikel bevat een opsomming van de taken van de Minister (ingevolge de huidige portefeuilleverdeling de Staatssecretaris) van Veiligheid en Justitie op het terrein van cybersecurity, ten behoeve waarvan verwerking van onder meer persoonsgegevens aangewezen is, en omschrijft de doeleinden van die taken. Zie voor een nadere toelichting hierop paragraaf 3 van het algemeen deel van deze memorie.

De in het eerste lid van dit artikel vermelde taken (bijstand, etc.) hebben telkens betrekking op (aanwijzingen voor) dreigingen en incidenten met betrekking tot de informatiesystemen van vitale aanbieders en andere van de rijksoverheid deel uitmakende aanbieders. Tot de doelgroep van het NCSC behoren derhalve primair de vitale aanbieders (overheid en ondernemingen) en alle andere aanbieders die onderdeel zijn van de rijksoverheid. Daarnaast kan over genoemde dreigingen en incidenten ook aan anderen advies of informatie worden verstrekt. Voor de in onderdeel c bedoelde analyses en technisch onderzoek geldt dat het verrichten enkel plaats kan vinden ten behoeve van de in de onderdelen a (bijstand) en b (advisering). In dit kader wordt nadrukkelijk geen onderzoek gedaan naar personen of organisaties die voor bovengenoemde dreigingen of incidenten verantwoordelijk zijn of anderszins daaraan bijdragen of hebben bijgedragen, zoals het achterhalen van de identiteit van dergelijke personen en organisaties.

Bij het verrichten van analyses en technisch onderzoek door het NCSC naar aanleiding van (aanwijzingen voor) dreigingen en incidenten met betrekking tot informatiesystemen van vitale aanbieders of van andere aanbieders die deel uitmaken van de rijksoverheid kunnen ook gegevens aan het licht komen over dreigingen of incidenten met betrekking tot andere informatiesystemen («bijvangst»). Ter voorkoming van nadelige maatschappelijke gevolgen regelt het tweede lid dat het NCSC ook als taak heeft laatstbedoelde gegevens in voorkomende gevallen in een beperkte kring van derden te delen ten behoeve van de informatievoorziening van andere organisaties of het publiek. Hierbij kan het ook gaan om persoonsgegevens, zoals e-mailadressen die door een ICT-inbreuk kwetsbaar zijn geworden. Verstrekking van de «bijvangst» kan krachtens het tweede lid onder meer geschieden aan organisaties die tot taak hebben (objectief kenbaar, bijvoorbeeld blijkend uit een wettelijk voorschrift of uit statuten) om andere organisaties te informeren over ICT-dreigingen en incidenten. Een voorbeeld van een dergelijke organisatie is SIDN, de Stichting Internet Domeinnaamregistratie Nederland (www.sidn.nl).
Voor de toepassing van de artikelen 2, tweede lid, en 9, tweede lid, zullen bij ministeriële regeling computercrisisteams worden aangewezen, na toetsing of gegevensuitwisseling daarmee gerechtvaardigd en verantwoord is. Het kan gaan om een aanwijzing van een individueel computercrisisteam of van een categorie van computercrisisteams.

**Artikel 3**

Bij de in dit artikel bedoelde (persoons)gegevens gaat het bijvoorbeeld om bij een incident of dreiging betrokken IP-adressen en om contactgegevens van vitale organisaties of andere organisaties binnen de rijks-

overheid en van andere melders van incidenten of kwetsbaarheden. Contactgegevens worden verwerkt om het NCSC onder meer in staat te stellen contact op te nemen met de meldende organisatie teneinde advies en ondersteuning te bieden. IP-adressen maken vaak deel uit van incident-informatie; op basis daarvan kan onderzoek worden gedaan naar de (ernst van de) inbreuk en kan advies over te treffen beveiligingsmaatregelen worden gegeven. Ook is deze kennis van belang ten behoeve van het informeren van derden, waaronder andere aanbieders, daar zij op basis van deze informatie alert kunnen worden gemaakt voor gelijksoortige inbreuken. Persoonsgegevens worden door het NCSC uiteraard verwerkt met inachtneming van de Wbp; zie ook paragraaf 6 van het algemeen deel van deze memorie. De Autoriteit persoonsgegevens alsook de departementale functionaris voor de gegevensbescherming houdt toezicht op deze verwerkingen door het NCSC. Uit de Wbp volgt onder andere dat persoonsgegevens die niet langer noodzakelijk zijn voor de uitoefening van de NCSC-taken zullen worden vernietigd. Ook andere gegevens, zoals vertrouwelijke bedrijfsgegevens, zullen worden vernietigd zodra de verwerking daarvan niet meer noodzakelijk is voor de uitoefening van die taken.

**Artikel 4**

Het eerste lid voorziet in een wettelijke bevoegdheid voor het NCSC om rechtspersonen (overheden of private partijen) of organen daarvan om gegevens te vragen die noodzakelijk zijn voor de uitoefening van de in artikel 2, eerste lid, genoemde taken. De taak, genoemd in het tweede lid van artikel 2, ziet alleen op verstrekking van gegevens door het NCSC aan derden en kan dus geen grondslag bieden voor verstrekking van gegevens aan het NCSC.
Het gaat bij de in het eerste lid geregelde bevoegdheid niet om een bevoegdheid tot het vorderen van gegevens; de rechtspersoon of het orgaan daarvan waaraan het verzoek is gericht is niet verplicht tot medewerking. Een dergelijke verplichting acht ik alleen nodig voor een krachtens artikel 5 aangewezen vitale aanbieder die bij het NCSC een meldplichtige ICT-inbreuk heeft gemeld; daarin voorziet artikel 7.
Voor de goede uitoefening van zijn taken is het van belang dat het NCSC, met het oog op het belang van voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van informatiesystemen van vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid, over voldoende gegevens beschikt over incidenten en kwetsbaarheden met betrekking tot informatiesystemen van de rijksoverheid en vitale private partijen. Het kan daarbij ook gaan om persoonsgegevens zoals IP-adressen (zie par. 6 van het algemeen deel). Ingevolge artikel 9, eerste lid, Wbp, mogen persoonsgegevens niet aan het NCSC worden verstrekt als dat onverenigbaar is met de doeleinden waarvoor die gegevens zijn verkregen. Op grond van artikel 43 Wbp kan de bevraagde organisatie artikel 9, eerste lid, buiten toepassing laten voor zover dit noodzakelijk is in het belang van onder meer de veiligheid van de Staat, gewichtige economische en financiële belangen van de Staat en andere openbare lichamen en de bescherming van de rechten en vrijheden van anderen. Artikel 43 Wbp biedt onvoldoende ruimte om artikel 9, eerste lid, Wbp buiten toepassing te laten in alle gevallen waarin het NCSC de persoonsgegevens nodig heeft voor de vervulling van de taken, genoemd in artikel 2, eerste lid, van dit wetsvoorstel, met name als de verstrekking aan het NCSC noodzakelijk is ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van elektronische informatiesystemen van vitale aanbieders die niet behoren tot de rijksoverheid (zie de aanhef van artikel 2, eerste lid). Een dergelijke verdere verwerking zal lang niet altijd gerechtvaardigd worden door het belang van de «veiligheid van de staat» of «gewichtige economische en

financiële belangen van de staat en andere openbare lichamen» (onderdelen a en c van artikel 43 Wbp). Gezien de NCSC-taken zullen de belangen «de voorkoming, opsporing en vervolging van strafbare feiten», «het toezicht op de naleving van wettelijke voorschriften die zijn gesteld ten behoeve van de belangen, bedoeld onder b en c» en «de bescherming van de betrokkene» (onderdelen b, d en e (eerste gedeelte) van artikel 43) geen rechtvaardiging bieden voor verstrekking van persoonsgegevens aan het NCSC. Op het eerste gezicht zou een verdere verwerking als hier bedoeld wellicht verdedigd kunnen worden op de grond dat zij noodzakelijk is ter bescherming van «de rechten en vrijheden van anderen» (artikel 43, onder e, Wbp), maar dat zou een ruime uitleg van deze restgrond vergen, terwijl artikel 43 bedoeld is voor uitzonderlijke omstandigheden en restrictief geïnterpreteerd moet worden (Kamerstukken II 1997/98, 25 892, nr. 3, p. 92). Naar mijn oordeel rechtvaardigt het zwaarwegende algemene belang dat het NCSC zijn wettelijke taken kan vervullen, de voorgestelde afwijking van de Wbp. Daarom stel ik voor om in het tweede lid van artikel 4 te bepalen dat het eerste lid van artikel 9 Wbp niet van toepassing is op de verstrekking van persoonsgegevens ingevolge een verzoek als bedoeld in artikel 4, eerste lid. Aangezien het NCSC gegevens verwerkt met het oog op (onder meer) het behartigen van de openbare veiligheid is deze afwijking van de Wbp niet in strijd met de Europese privacyrichtlijn (artikelen 3, tweede lid, eerste streepje, en 13, eerste lid, onder c).[36] De vertrouwelijkheid van de gegevens die op grond van artikel 4 worden verstrekt aan het NCSC wordt beschermd door artikel 9 van dit wetsvoorstel.

**Artikel 5**

Dit artikel geeft een grondslag voor aanwijzing bij algemene maatregel van bestuur (amvb) van de vitale aanbieders en de door hen aangeboden producten en diensten waarvoor de in artikel 6 opgenomen meldplicht geldt en de in artikel 7 opgenomen verplichting om na een verplichte melding desgevraagd nadere gegevens te verstrekken. Het kan daarbij gaan om de aanwijzing van individuele aanbieders of om de aanwijzing van categorieën van aanbieders (bijvoorbeeld «drinkwaterbedrijven als bedoeld in de Drinkwaterwet» of «de bij besluit van De Nederlandsche Bank N.V. aangewezen financiële instellingen»). Het moet gaan om voor de Nederlandse samenleving vitale producten of diensten, zie de omschrijving van «vitale aanbieder» in artikel 1. Een meldplichtige aanbieder kan op zich ook buiten Nederland gevestigd zijn; het gaat erom dat hij producten of diensten aanbiedt die van vitaal belang zijn voor de Nederlandse samenleving. De betrokken sectoren zullen over de amvb worden geconsulteerd. De voordracht voor de amvb zal worden gedaan in overeenstemming met de andere betrokken bewindspersonen.

**Artikel 6**

De meldplicht geldt alleen als voldaan is aan de volgende cumulatieve voorwaarden:

1. Het gaat om een krachtens artikel 5 aangewezen product of dienst van een krachtens datzelfde artikel aangewezen vitale aanbieder.
2. Er is of was een daadwerkelijke inbreuk op de veiligheid of een daadwerkelijk verlies van integriteit van een elektronisch informatiesysteem waarvan het product of de dienst afhankelijk is.

[36] Richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995, L 281).

3. Die inbreuk of dat verlies heeft geleid, of kan leiden tot een onderbreking van de beschikbaarheid of de betrouwbaarheid van het product of de dienst.
4. Die feitelijke of potentiële onderbreking moet belangrijk zijn, dus substantieel.

Doordat de meldplicht alleen geldt als de onderbreking van de beschikbaarheid of de betrouwbaarheid wordt veroorzaakt door een inbreuk op de veiligheid of door een verlies van integriteit, valt een onderbreking van de beschikbaarheid door een DDos-aanval buiten de meldplicht. Een dergelijke aanval gaat immers niet gepaard met een inbreuk op de veiligheid of een verlies van integriteit.

Mede op basis van overleg met de betrokken sectoren en departementen zal nader worden uitgewerkt, en bijvoorbeeld in richtsnoeren worden vastgelegd, wat voor de verschillende betrokken producten en diensten moet worden verstaan onder «in belangrijke mate». Daarbij zal mede bepalend zijn onder welke omstandigheden sprake is of kan zijn van maatschappelijke ontwrichting. Hierbij gaat het bijvoorbeeld om een criterium als de langdurigheid van de uitval van een vitaal proces of vitale dienst waarmee de getroffen organisatie alsook andere partijen geconfronteerd wordt. Tevens valt te denken aan een criterium als de ernst en de omvang van de uitval van een vitaal proces of vitale dienst, waaronder de mate waarin ook andere organisaties of het publiek schade hiervan ondervinden.

De meldplicht geldt dus ook als de ICT-inbreuk nog niet daadwerkelijk heeft geleid tot een belangrijke onderbreking van de beschikbaarheid of betrouwbaarheid van een vitaal product of vitale dienst, maar dat gevolg wel alsnog kan hebben. Dit is immers evenzeer informatie die van groot belang is met het oog op het beperken of voorkomen van schadelijke maatschappelijke gevolgen. Bovendien kan ook van dergelijke inbreuken veel worden geleerd.

Van belang is het dat de melding van een ICT-inbreuk waarvoor de meldplicht geldt zo spoedig mogelijk wordt gedaan. Daarbij dient in aanmerking genomen te worden dat soms enige tijd zal verstrijken tussen de feitelijke inbreuk en de constatering (van de ernst) daarvan door de getroffen organisatie. Het is belangrijk dat het NCSC zo snel mogelijk in staat wordt gesteld om te beoordelen of en in welke zin de getroffen aanbieder door het NCSC moet worden bijgestaan bij het treffen van maatregelen om de beschikbaarheid en betrouwbaarheid van het vitale product of de vitale dienst te waarborgen, en om de risico's van de gemelde inbreuk in te schatten voor de informatiesystemen van andere aanbieders. Daartoe kan overigens zo nodig op grond van artikel 7 van dit wetsvoorstel door het NCSC aan de meldende vitale aanbieder om aanvullende informatie worden gevraagd. De initiële melding kan beknopt zijn: liever een snelle melding die zo nodig later kan worden aangevuld, dan een uitvoerige melding die daardoor op zich laat wachten. Zie ook paragraaf 2.2.

De omschrijving van de bij de melding te verstrekken gegevens is zo veel mogelijk identiek aan de omschrijving in artikel 7, tweede lid, van het Besluit continuïteit openbare elektronische communicatienetwerken en -diensten en aan de omschrijving die voor verleners van gekwalificeerde certificaten is opgenomen in artikel 2, eerste lid, onder q, van het Besluit elektronische handtekeningen. Het gaat hierbij om gegevens die het NCSC in ieder geval nodig heeft voor een goede uitoefening van zijn taken.

Gemeld zal onder meer een prognose van de hersteltijd moeten worden. Wat de benodigde hersteltijd betreft moet, voor zover van toepassing, onderscheid worden gemaakt tussen enerzijds de tijd die nodig is voor het herstel van de meest essentiële onderdelen van het bedrijfsproces met mogelijke alternatieve of tijdelijke noodvoorzieningen teneinde de continuïteit van de beschikbaarheid of betrouwbaarheid van een voor de samenleving vitale dienst of vitaal product te garanderen, en anderzijds het volledig herstel van de bij de inbreuk betrokken informatiesystemen van de betrokken vitale aanbieder en het volledig hervatten van alle processen binnen de organisatie van deze aanbieder, met inbegrip van het wegwerken van eventueel opgelopen achterstanden.

**Artikel 7**

Denkbaar is dat het NCSC naar aanleiding van een melding nadere gegevens nodig heeft om de getroffen organisatie adequaat te kunnen helpen, bijvoorbeeld als deze bij het doen van de melding nog geen zekerheid kon bieden over de gevolgen van de inbreuk of over de te nemen maatregelen. Ook kunnen nadere gegevens nodig zijn om de risico's te kunnen inschatten voor informatiesystemen van de andere aanbieders die tot de doelgroep van het NCSC behoren. Dit artikel bevat voor dergelijke gevallen een aanvullende informatieplicht, die wordt geactiveerd door een concreet verzoek van het NCSC in reactie op een in artikel 6 bedoelde melding.

**Artikel 8**

Dit artikel bevat de grondslag om, indien nodig, nadere regels te stellen over bijvoorbeeld de gegevens die in het kader van de meldplicht moeten worden verstrekt of om te verduidelijken wat voor de verschillende aangewezen producten en diensten bij de toepassing van artikel 6, eerste lid, moet worden verstaan onder «in belangrijke mate». De betrokken sectoren zullen over de nadere regels worden geconsulteerd.

**Artikel 9**

Dit artikel regelt de verstrekking door het NCSC aan derden van vertrouwelijke gegevens met betrekking tot aanbieders die het NCSC heeft verkregen, zoals gegevens over de identiteit van een bij een incident betrokken aanbieder of specifieke gegevens over de beveiliging van een elektronisch informatiesysteem van een aanbieder. Zie hierover ook paragraaf 4 van het algemeen deel van deze memorie. Artikel 9 ziet op alle vertrouwelijke gegevens met betrekking tot aanbieders die zich bij het NCSC bevinden, en is dus niet beperkt tot de gegevens die het NCSC heeft verkregen op grond van de in artikel 6 bedoelde meldplicht of naar aanleiding van een verzoek als bedoeld in artikel 7.

De medewerkers van het NCSC zijn gebonden aan de geheimhoudingsplicht van artikel 272 van het Wetboek van Strafrecht en artikel 2:5 van de Algemene wet bestuursrecht. Deze laatste bepaling geldt voor «Een ieder die is betrokken bij de uitvoering van de taak van een bestuursorgaan en daarbij de beschikking krijgt over gegevens waarvan hij het vertrouwelijke karakter kent of redelijkerwijs moet vermoeden». De geheimhoudingsplicht geldt niet «voor zover enig wettelijk voorschrift hem tot mededeling verplicht of uit zijn taak de noodzaak tot mededeling voortvloeit». Uit de NCSC-taken in artikel 2 kan de noodzaak voortvloeien tot mededeling van vertrouwelijke gegevens met betrekking tot aanbieders. Artikel 9 regelt onder welke voorwaarden en aan wie dergelijke gegevens mogen worden verstrekt ter uitvoering van de NCSC-taken.

Het eerste lid is mede ontleend aan de artikelen 1:90, eerste lid, onderdelen d en f, en 1:93, tweede lid, onderdelen d en f, van de Wet op het financieel toezicht (verstrekking van vertrouwelijke gegevens door de toezichthouder). Deze bepaling regelt dat bij het NCSC, bijvoorbeeld naar aanleiding van een melding, berustende vertrouwelijke gegevens slechts ter uitvoering van de in artikel 2 genoemde taken aan derden worden verstrekt, indien aldaar de geheimhouding van de gegevens voldoende is gewaarborgd en voldoende is gewaarborgd dat de gegevens uitsluitend worden gebruikt voor het doel waarvoor zij worden verstrekt.

Het eerste lid ziet op vertrouwelijke gegevens met betrekking tot aanbieders, dus niet op andere vertrouwelijke gegevens, zoals persoonsgegevens die niet herleidbaar zijn tot een aanbieder (bijvoorbeeld de e-mailadressen die op grond van artikel 2, tweede lid, voor verstrekking aan derden in aanmerking komen). Voor de verwerking van laatstbedoelde persoonsgegevens door het NCSC geldt de Wbp, net als voor de verwerking van andere persoonsgegevens waarover het NCSC beschikt. Soms zijn gegevens die betrekking hebben op een aanbieder vertrouwelijk zonder dat zij tot die aanbieder herleid kunnen worden. Denk aan een nieuw concurrentiegevoelig bedrijfsprocedé dat buiten de betrokken onderneming nog niet bekend is. Anders dan het tweede, derde en vierde lid ziet het eerste lid ook op dergelijke vertrouwelijke maar niet-herleidbare gegevens.

Zowel het eerste lid als het tweede lid zien alleen op verstrekking van de daarin bedoelde vertrouwelijke gegevens «ter uitvoering van de in artikel 2 genoemde taken», en dus niet op verplichtingen tot verstrekking door het NCSC van vertrouwelijke gegevens uit hoofde van andere wetten,[37] zoals artikel 8:28 Algemene wet bestuursrecht (inlichtingen verstrekken aan de bestuursrechter door partijen in een beroepsprocedure) of artikel 126nc e.v. Wetboek van Strafvordering (vorderen van gegevens door officier van justitie).

Uit het tweede lid volgt dat verstrekking, uit hoofde van artikel 2, van vertrouwelijke gegevens die herleid kunnen worden tot een aanbieder, zonder diens instemming alleen mogelijk is aan computercrisisteams die bij ministeriële regeling zijn aangewezen en aan de Nederlandse inlichtingen- en veiligheidsdiensten, en dan alleen voor zover dat dienstig is voor het bevorderen van maatregelen ter voorkoming of beperking van een verstoring van het maatschappelijk verkeer. Als de aanbieder daar toestemming voor geeft, dan kunnen de gegevens uiteraard ook aan andere organisaties worden verstrekt, bijvoorbeeld aan een sectorale toezichthouder. Een dergelijke toestemming kan bijvoorbeeld overleg mogelijk maken tussen het NCSC en die toezichthouder om te voorkomen dat de aanbieder geconfronteerd wordt met een aanwijzing van de toezichthouder die tegenstrijdig is aan het advies van het NCSC (zie voorlaatste alinea par. 2.5). De formulering «gegevens die herleid kunnen worden tot een aanbieder» doelt op de naam van een aanbieder en alle andere gegevens waarmee in redelijkheid de identiteit van die aanbieder direct dan wel indirect kan worden vastgesteld.

Gelet op de in artikel 2 genoemde taken heeft het NCSC het (mede) tot taak om vitale aanbieders en andere aanbieders die onderdeel zijn van de rijksoverheid te adviseren over maatregelen die zouden kunnen worden genomen vanwege een dreiging of incidenten met betrekking tot hun informatiesystemen. Een dergelijk advies is niet bindend. Het is echter onwenselijk als de betrokken aanbieder zich vrij voelt om het advies

[37] Vgl. «voor zover enig wettelijk voorschrift hem tot mededeling verplicht» in artikel 2:5 Algemene wet bestuursrecht.

zonder goede reden naast zich neer te leggen. Het derde lid beoogt dat te voorkomen.[38] Het blijft primair de eigen verantwoordelijkheid van de aanbieder zelf om passende maatregelen te nemen om uitval of verstoring van zijn product of dienst te voorkomen of te beperken. Ook is het primair aan de aanbieder zelf om, als een wettelijk voorschrift hiertoe verplicht, de eigen toezichthouders of vakdepartementen op de hoogte te stellen. Voor het geval de Staatssecretaris van Veiligheid en Justitie echter van oordeel is dat de aanbieder onvoldoende gevolg geeft aan het advies, en daardoor het risico op maatschappelijke ontwrichting aanwezig blijft, kan hij de voor de betrokken sector verantwoordelijke Minister of Staatssecretaris dat advies, met inbegrip van de daarin opgenomen herleidbare gegevens, verstrekken (artikel 9, derde lid). Wanneer het voornemen bestaat om in een dergelijk geval een advies door te zenden aan een betrokken bewindspersoon, zal het NCSC daarover in overleg treden met het betrokken ministerie. Na doorzending zal het NCSC, indien gewenst, het betrokken ministerie nader informeren en adviseren over de cybersecurity-aspecten van het incident of de kwetsbaarheid waarop het advies betrekking heeft.

Als het advies betrekking heeft op een rijksoverheidsorganisatie zal in elk geval (ook) de Minister van Binnenlandse Zaken en Koninkrijksrelaties worden geïnformeerd, aangezien hij in elk geval «betrokken» (in de zin van het derde lid) is, gezien zijn coördinerende rol voor informatiesystemen van de overheid.
Wat betreft verstrekking van herleidbare gegevens aan sectorale toezichthouders ziet het derde lid uitsluitend op toezichthoudende diensten die onderdeel zijn van een ministerie. Verstrekking aan andere toezichthouders kan alleen op grond van het vierde lid, onderdeel b.
De aanbieder heeft voldoende gevolg gegeven aan het advies als hij het advies weliswaar niet heeft gevolgd, maar de dreiging niettemin in voldoende mate is verdwenen, bijvoorbeeld doordat de organisatie andere dan de geadviseerde maatregelen heeft genomen of door adequate actie van anderen.
De verstrekking van het NCSC-advies aan de eerstverantwoordelijke bewindspersoon is een feitelijke handeling. De beslissing tot verstrekking is geen besluit in de zin van de Algemene wet bestuursrecht vanwege het ontbreken van rechtsgevolg: de verstrekking brengt geen wijziging in de rechten of plichten van de betrokken aanbieder en het advies wordt ook niet openbaar gemaakt. Het is aan de eerstverantwoordelijke bewindspersoon om al dan niet actie te ondernemen naar aanleiding van het aan hem verstrekte NCSC-advies. Tegen de (beslissing tot) verstrekking staat dan ook geen bestuursrechtelijke rechtsbescherming open.

Het vierde lid ziet op het specifieke geval dat verstrekking van bovenbedoelde herleidbare gegevens nodig is om ernstige maatschappelijke gevolgen te voorkomen of te beperken. In een dergelijk geval is het NCSC verplicht om die gegevens te verstrekken aan de politiek verantwoordelijke bewindspersoon of -personen (onderdeel a). Daarbij kan bijvoorbeeld worden gedacht aan een dreigende crisissituatie ten aanzien waarvan het nemen van crisisbeheersingsmaatregelen aangewezen kan zijn.
Aan andere organisaties of aan het publiek mogen dergelijke gegevens met toepassing van het vierde lid slechts worden verstrekt na raadpleging van de betrokken aanbieder (onderdeel b). Daarbij spreekt het voor zich dat deze informatieverstrekking niet verder gaat dan strikt noodzakelijk is om die organisaties of het publiek in staat te stellen om te bepalen of en welke maatregelen zij in dit verband dienen te nemen. Voor dit doel zal het in beginsel slechts in uitzonderlijke gevallen nodig zijn om herleidbare gegevens te verstrekken. De formulering «andere organisaties» ziet

[38] Kamerstukken II 2013/14, 26 643, nr. 297, p. 4.

bijvoorbeeld ook op een toezichthoudende dienst die geen onderdeel is van een ministerie, zoals De Nederlandse Bank of de Autoriteit Financiële Markten.

Op de verstrekking, op grond van het vierde lid, van herleidbare gegevens aan het publiek is reeds ingegaan in het algemeen deel van deze memorie (paragraaf 4). Omdat dergelijke mededelingen naar hun aard niet samengaan met geheimhouding en doelbinding, bepaalt het vijfde lid dat het eerste lid op die mededelingen niet van toepassing is.

Zoals uiteengezet in het algemeen deel van deze memorie bevat artikel 9 een bijzondere openbaarheidsregeling voor vertrouwelijke herleidbare gegevens die afwijkt van de Wet openbaarheid van bestuur. Het zesde lid stelt dit buiten twijfel. Deze afwijking geldt niet alleen zolang die gegevens bij het NCSC berusten, maar ook nadat zij, na verstrekking door het NCSC op grond van artikel 9, bij een ander overheidsorgaan berusten.

Een en ander geldt echter niet voor milieu-informatie. Ter uitvoering van het Verdrag van Aarhus[39] en EU-richtlijn 2003/4/EG[40] bevat de Wob voor het verstrekken van milieu-informatie diverse afwijkende bepalingen. Zo is de weigeringsgrond voor bedrijfs- en fabricagegegevens die vertrouwelijk aan de overheid zijn meegedeeld in het geval van milieu-informatie niet absoluut[41] maar relatief,[42] en in plaats van de relatieve weigeringsgrond dat onevenredige bevoordeling of benadeling voorkomen moet worden[43] geldt voor milieu-informatie dat verstrekking achterwege blijft voor zover het belang daarvan niet opweegt tegen de bescherming van het milieu waarop de informatie betrekking heeft of de beveiliging van bedrijven en het voorkomen van sabotage.[44] Hoewel herleidbare gegevens in de meeste gevallen zelf geen informatie over het milieu bevatten, blijkt uit de rechtspraak dat namen van ondernemingen milieu-informatie kunnen inhouden als zij onlosmakelijk verbonden zijn met maatregelen en activiteiten ter bescherming van elementen van het milieu.[45] Om strijdigheid met het genoemde verdrag en de genoemde richtlijn te voorkomen, volgt uit het zesde lid van artikel 9 dat de Wob onverkort van toepassing is op herleidbare gegevens die milieu-informatie inhouden.

Artikel 9, en dan met name het eerste lid, staat er niet aan in de weg dat het NCSC vertrouwelijke gegevens die *niet* herleidbaar zijn, uit eigen beweging verstrekt aan bijvoorbeeld de politie en het openbaar ministerie in de reeds bestaande overlegstructuren. Wél herleidbare gegevens kunnen door het NCSC aan politie en OM worden verstrekt als de betrokken aanbieder daarmee instemt. Beide vormen van verstrekking kunnen voor de officier van justitie vervolgens aanleiding zijn om gebruik te maken van zijn wettelijke bevoegdheid om bij het NCSC gegevens te vorderen.

---

[39] Verdrag betreffende toegang tot informatie, inspraak bij besluitvorming en toegang tot de rechter inzake milieuaangelegenheden, Trb. 2001, 73.
[40] Richtlijn 2003/4/EG van het Europees Parlement en de Raad van 28 januari 2003 inzake de toegang van het publiek tot milieu-informatie en tot intrekking van Richtlijn 90/313/EEG van de Raad, PbEU 2003, L 41).
[41] Artikel 10, eerste lid, aanhef en onder c, Wob.
[42] Artikel 10, vierde lid, tweede volzin, Wob.
[43] Artikel 10, tweede lid, aanhef en onder g, Wob.
[44] Artikel 1, onder g, en artikel 10, zesde en zevende lid, Wob.
[45] ABRvS 10 maart 2010, ECLI:NL:RVS:2010:BL7035.

## Artikel 10

Hoewel het in de bedoeling ligt om deze wet als één geheel in werking te laten treden, is de mogelijkheid van gedifferentieerde inwerkingtreding opengehouden. De bepaling is overigens niet bedoeld om de meldplicht van artikel 6, eerste lid, voor afzonderlijke organisaties, producten of diensten op verschillende tijdstippen in werking te kunnen laten treden. Mocht een dergelijke differentiatie nodig zijn, dan kan zij eventueel worden vormgegeven in de algemene maatregel van bestuur, bedoeld in artikel 5.

De Staatssecretaris van Veiligheid en Justitie,
K.H.D.M. Dijkhoff